vShield Administration Guide

vShield Manager 5.5
vShield App 5.5
vShield Edge 5.5
vShield Endpoint 5.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001280-03

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2010 – 2015 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

vShield Administration Guide 13

1 Overview of vShield 15
- About vShield Components 15
- Migration of vShield Components 17
- About VMware Tools on vShield Components 17
- Ports Required for vShield Communication 17

2 vShield Manager User Interface Basics 19
- Log in to the vShield Manager User Interface 19
- About the vShield Manager User Interface 20
  - vShield Manager Inventory Panel 20
  - vShield Manager Configuration Panel 21

3 Management System Settings 23
- Edit DNS Servers 23
- Edit the vShield Manager Date and Time 24
- Edit Lookup Service Details 24
- Edit vCenter Server 24
- Specify Syslog Server 25
- Download Technical Support Logs for vShield 25
- Add an SSL Certificate to Identify the vShield Manager Web Service 26
  - Import an SSL certificate 26
- Working with Services and Service Groups 27
  - Create a Service 27
  - Create a Service Group 28
  - Edit a Service or Service Group 28
  - Delete a Service or Service Group 29
- Grouping Objects 30
  - Working with IP Address Groups 30
  - Working with MAC Address Groups 32
  - Working with Security Groups 34

4 User Management 37
- Configure Single Sign On 37
- Managing User Rights 38
- Managing the Default User Account 39
- Add a User Account 39
- Edit a User Account 41
- Change a User Role 41
- Disable or Enable a User Account 42

Delete a User Account 42

5 Updating System Software 43
View the Current System Software 43
Upload an Update 43

6 Backing Up vShield Manager Data 45
Back Up Your vShield Manager Data on Demand 45
Schedule a Backup of vShield Manager Data 46
Restore a Backup 46

7 System Events and Audit Logs 49
View the System Event Report 49
vShield Manager Virtual Appliance Events 49
vShield App Events 50
About the Syslog Format 51
View the Audit Log 51

8 VXLAN Virtual Wires Management 53
Preparing your Network for VXLAN Virtual Wires 54
Associating Clusters with Distributed Switches 54
Assign Segment ID Pool and Multicast Address Range to vShield Manager 55
Create a VXLAN Virtual Wire 55
Add a Network Scope 55
Add a VXLAN Virtual Wire 56
Connect a VXLAN Virtual Wire to a vShield Edge 56
Deploy Services on a VXLAN Virtual Wire 57
Connect Virtual Machines to a VXLAN Virtual Wire 57
Test VXLAN Virtual Wire Connectivity 58
Viewing Flow Monitoring Data for a VXLAN Virtual Wire 59
Working with Firewall Rules for VXLAN Virtual Wires 59
Prevent Spoofing on a VXLAN Virtual Wire 60
Editing Network Scopes 60
View and Edit a Network Scope 60
Expand a Network Scope 60
Contract a Network Scope 61
Edit a VXLAN Virtual Wire 61
Sample Scenario for Creating VXLAN Virtual Wires 62
John Admin Associates Cluster with Distributed Switches 64
John Admin Assigns Segment ID Pool and Multicast Address Range to vShield Manager 65
John Admin Adds a Network Scope 65
John Admin Adds a VXLAN Virtual Wire 65

9 vShield Edge Management 67
View the Status of a vShield Edge 68
Configure vShield Edge Settings 68
Managing Appliances 68
Add an Appliance 68

Change an Appliance 69
Delete an Appliance 69
Working with Interfaces 70
Add an Interface 70
Change Interface Settings 71
Delete an Interface 71
Enable an Interface 72
Disable an Interface 72
Working with Certificates 73
Configure a CA Signed Certificate 73
Configure a Self-Signed Certificate 74
Using Client Certificates 75
Add a Certificate Revocation List 75
Managing the vShield Edge Firewall 76
Add a vShield Edge Firewall Rule 76
Change Default Firewall Rule 79
Change a vShield Edge Firewall Rule 80
Change the Priority of a vShield Edge Firewall Rule 80
Delete a vShield Edge Firewall Rule 80
Managing NAT Rules 81
Add a SNAT Rule 81
Add a DNAT Rule 82
Working with Static Routes 83
Set the Default Gateway 83
Add a Static Route 83
Managing DHCP Service 84
Add a DHCP IP Pool 84
Add a DHCP Static Binding 85
Managing VPN Services 86
IPSec VPN Overview 86
SSL VPN-Plus Overview 109
Managing Load Balancer Service 140
Configure Load Balancer Service 140
Edit a Server Pool 143
Delete a Server Pool 144
Edit a Virtual Server 144
Delete a Virtual Server 144
About High Availability 145
Change HA Configuration 146
Configure DNS Servers 146
Configure Remote Syslog Servers 147
Change CLI Credentials 147
Upgrade vShield Edge to Large or X-Large 147
Download Tech Support Logs for vShield Edge 148
Synchronize vShield Edge with vShield Manager 148
Redeploy vShield Edge 149

10 Service Insertion Management 151
Inserting a Network Services 151
Register Service Manager 152
Register Service 152
Create Service Profiles 153
Deploy Service 154
Change Service Precedence 154
Edit a Service Manager 154
Delete a Service Manager 155
Edit a Service 155
Delete a Service 155
Edit a Service Profile 155
Delete a Service Profile 156

11 vShield App Management 157
Sending vShield App System Events to a Syslog Server 157
Viewing the Current System Status of a vShield App 158
Restart a vShield App 158
Forcing a vShield App to Synchronize with the vShield Manager 158
Viewing Traffic Statistics by vShield App Interface 159
Download Technical Support Logs for vShield App 159
Configuring Fail Safe Mode for vShield App Firewall 159
Excluding Virtual Machines from vShield App Protection 159

12 vShield App Flow Monitoring 161
Viewing the Flow Monitoring Data 161
Add or Edit App Firewall Rule from the Flow Monitoring Report 164
Change the Date Range of the Flow Monitoring Charts 165

13 vShield App Firewall Management 167
Using App Firewall 167
Namespaces in a Multi Tenant Environment 167
About Services and Service Groups 168
Designing Security Groups 168
About System Defined Rules in App Firewall 168
About General and Ethernet Rules 168
Firewall Rules Precedence 168
Planning App Firewall Rule Enforcement 169
Working with Firewall Rules 169
Add a Firewall Rule 169
Delete a Firewall Rule 172
Revert to a Previous Firewall Configuration 173
Change the Order of a Rule 173
Using SpoofGuard 174
SpoofGuard Screen Options 175
Enable SpoofGuard 175
Approve IP Addresses 176
Edit an IP Address 176

Delete an IP Address 177

14 vShield Endpoint Events and Alarms 179
View vShield Endpoint Status 179
vShield Endpoint Alarms 180
Host Alarms 180
SVM Alarms 180
vShield Endpoint Events 180
vShield Endpoint Audit Messages 181

15 vShield Data Security Management 183
vShield Data Security User Roles 183
Defining a Data Security Policy 184
Select Regulations 184
Specify Areas Participating in the Policy Scan 185
Specify File Filters 185
Editing a Data Security Policy 186
Running a Data Security Scan 187
Viewing and Downloading Reports 187
Creating Regular Expressions 188
Available Regulations 188
Arizona SB-1338 188
ABA Routing Numbers 189
Australia Bank Account Numbers 189
Australia Business and Company Numbers 189
Australia Medicare Card Numbers 190
Australia Tax File Numbers 190
California AB-1298 190
California SB-1386 191
Canada Social Insurance Numbers 191
Canada Drivers License Numbers 191
Colorado HB-1119 192
Connecticut SB-650 192
Credit Card Numbers 192
Custom Account Numbers 192
EU Debit Card Numbers 193
FERPA (Family Educational Rights and Privacy Act) 193
Florida HB-481 193
France IBAN Numbers 193
France National Identification Numbers Policy 193
Georgia SB-230 Policy 194
Germany BIC Numbers Policy 194
Germany Driving License Numbers Policy 194
Germany IBAN Numbers Policy 194
Germany National Identification Numbers Policy 194
Germany VAT Numbers Policy 194
Hawaii SB-2290 Policy 195
HIPAA (Healthcare Insurance Portability and Accountability Act) Policy 195

Idaho SB-1374 Policy 195
Illinois SB-1633 196
Indiana HB-1101 Policy 196
Italy Driving License Numbers Policy 196
Italy IBAN Numbers Policy. 196
Italy National Identification Numbers Policy 196
Kansas SB-196 Policy 197
Louisiana SB-205 Policy 197
Maine LD-1671 Policy 197
Massachusetts CMR-201 198
Minnesota HF-2121 198
Montana HB-732 198
Netherlands Driving Licence Numbers 198
Nevada SB-347 199
New Hampshire HB-1660 199
New Jersey A-4001 199
New York AB-4254 200
New Zealand Inland Revenue Department Numbers 200
New Zealand Ministry of Health Numbers 200
Ohio HB-104 200
Oklahoma HB-2357 201
Patient Identification Numbers 201
Payment Card Industry Data Security Standard (PCI-DSS) 201
Texas SB-122 201
UK BIC Numbers 202
UK Driving Licence Numbers 202
UK IBAN Numbers 202
UK National Health Service Numbers 202
UK National Insurance Numbers (NINO) 202
UK Passport Numbers 202
US Drivers License Numbers 203
US Social Security Numbers 203
Utah SB-69 203
Vermont SB-284 203
Washington SB-6043 203
Available Content Blades 204
ABA Routing Number Content Blade 204
Admittance and Discharge Dates Content Blade 204
Alabama Drivers License Content Blade 204
Alaska Drivers License Content Blade 204
Alberta Drivers Licence Content Blade 204
Alaska Drivers License Content Blade 205
Alberta Drivers Licence Content Blade 205
American Express Content Blade 205
Arizona Drivers License Content Blade 205
Arkansas Drivers License Content Blade 205
Australia Bank Account Number Content Blade 205
Australia Business Number Content Blade 206
Australia Company Number Content Blade 206

Australia Medicare Card Number Content Blade 206
Australia Tax File Number Content Blade 206
California Drivers License Number Content Blade 206
Canada Drivers License Number Content Blade 206
Canada Social Insurance Number Content Blade 206
Colorado Drivers License Number Content Blade 206
Connecticut Drivers License Number Content Blade 207
Credit Card Number Content Blade 207
Credit Card Track Data Content Blade 207
Custom Account Number Content Blade 207
Delaware Drivers License Number Content Blade 207
EU Debit Card Number Content Blade 207
Florida Drivers License Number Content Blade 208
France Driving License Number Content Blade 208
France BIC Number Content Blade 208
France IBAN Number Content Blade 208
France National Identification Number Content Blade 208
France VAT Number Content Blade 208
Georgia Drivers License Number Content Blade 208
Germany BIC Number Content Blade 208
Germany Driving License Number Content Blade 209
Germany IBAN Number Content Blade 209
Germany National Identification Numbers Content Blade 209
Germany Passport Number Content Blade 209
Germany VAT Number Content Blade 209
Group Insurance Numbers Content Blade 209
Hawaii Drivers License Number Content Blade 209
Italy National Identification Numbers Content Blade 209
Health Plan Beneficiary Numbers 210
Idaho Drivers License Number Content Blade 210
Illinois Drivers License Number Content Blade 210
Indiana Drivers License Number Content Blade 210
Iowa Drivers License Number Content Blade 211
Index of Procedures Content Blade 211
Italy Driving License Number Content Blade 211
Italy IBAN Number Content Blade 211
ITIN Unformatted Content Blade 212
Kansas Drivers License Number Content Blade 212
Kentucky Drivers License Number Content Blade 212
Louisiana Drivers License Number Content Blade 212
Maine Drivers License Number Content Blade 212
Manitoba Drivers Licence Content Blade 212
Maryland Drivers License Number Content Blade 213
Massachusetts Drivers License Number Content Blade 213
Michigan Drivers License Number Content Blade 213
Minnesota Drivers License Number Content Blade 213
Mississippi Drivers License Number Content Blade 213
Missouri Drivers License Number Content Blade 213
Montana Drivers License Number Content Blade 214

NDC Formulas Dictionary Content Blade 214
Nebraska Drivers License Number Content Blade 214
Netherlands Driving Licence Number Content Blade 214
Netherlands IBAN Number Content Blade 214
Netherlands National Identification Numbers Content Blade 215
Netherlands Passport Number Content Blade 215
Nevada Drivers License Number Content Blade 215
New Brunswick Drivers Licence Content Blade 215
New Hampshire Drivers License Number Content Blade 215
New Jersey Drivers License Number Content Blade 215
New Mexico Drivers License Number Content Blade 216
New York Drivers License Number Content Blade 216
New Zealand Health Practitioner Index Number Content Blade 216
New Zealand Inland Revenue Department Number 216
New Zealand National Health Index Number Content Blade 216
Newfoundland and Labrador Drivers Licence Content Blade 216
North Carolina Drivers License Number Content Blade 216
North Dakota Drivers License Number Content Blade 216
Nova Scotia Drivers Licence Content Blade 217
Ohio Drivers License Number Content Blade 217
Oklahoma License Number Content Blade 217
Ontario Drivers Licence Content Blade 217
Oregon License Number Content Blade 217
Patient Identification Numbers Content Blade 217
Pennsylvania License Number Content Blade 217
Prince Edward Island Drivers Licence Content Blade 217
Protected Health Information Terms Content Blade 218
Quebec Drivers Licence Content Blade 218
Rhode Island License Number Content Blade 218
Saskatchewan Drivers Licence Content Blade 218
SIN Formatted Content Blade 218
SIN Unformatted Content Blade 219
SSN Formatted Content Blade 219
SSN Unformatted Content Blade 219
South Carolina License Number Content Blade 219
South Dakota License Number Content Blade 219
Spain National Identification Number Content Blade 219
Spain Passport Number Content Blade 219
Spain Social Security Number Content Blade 220
Sweden IBAN Number Content Blade 220
Sweden Passport Number Content Blade 220
Tennessee License Number Content Blade 220
UK BIC Number Content Blade 220
UK Driving License Number Content Blade 221
UK IBAN Number Content Blade 221
UK National Health Service Number Content Blade 221
UK NINO Formal Content Blade 222
UK Passport Number Content Blade 222
Utah License Number Content Blade 222

Virginia License Number Content Blade 222
Visa Card Number Content Blade 222
Washington License Number Content Blade 222
Wisconsin License Number Content Blade 222
Wyoming License Number Content Blade 223
Supported File Formats 223

16 Troubleshooting 229
Troubleshoot vShield Manager Installation 229
vShield OVA File Cannot Be Installed in vSphere Client 229
Cannot Log In to CLI After the vShield Manager Virtual Machine Starts 229
Cannot Log In to the vShield Manager User Interface 230
Troubleshooting Operational Issues 230
vShield Manager Cannot Communicate with a vShield App 230
Cannot Configure a vShield App 230
Firewall Block Rule Not Blocking Matching Traffic 231
No Flow Data Displaying in Flow Monitoring 231
Troubleshooting vShield Edge Issues 231
Virtual Machines Are Not Getting IP Addresses from the DHCP Server 231
Load-Balancer Does Not Work 232
Load-Balancer Throws Error 502 Bad Gateway for HTTP Requests 232
VPN Does Not Work 232
SSL VPN does Not Work 233
Troubleshoot vShield Endpoint Issues 233
Thin Agent Logging 233
Component Version Compatibility 233
Check vShield Endpoint Health and Alarms 234
Troubleshooting vShield Data Security Issues 234
Review Scan Start and Stop Timestamp 234
About Accuracy in Detecting Violations 234

Index 237

vShield Administration Guide

The *vShield Administration Guide* describes how to install, configure, monitor, and maintain the VMware® vShield™ system by using the vShield Manager user interface, and the vSphere Client plug-in. The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This manual is intended for anyone who wants to install or use vShield in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware Infrastructure 5.x, including VMware ESX, vCenter Server, and the vSphere Client.

1 Overview of vShield

VMware® vShield is a suite of security virtual appliances built for VMware vCenter Server and VMware ESX integration. vShield is a critical security component for protecting virtualized datacenters from attacks and helping you achieve your compliance-mandated goals.

This guide assumes you have administrator access to the entire vShield system. The viewable resources in the vShield Manager user interface can differ based on the assigned role and rights of a user, and licensing. If you are unable to access a screen or perform a particular task, consult your vShield administrator.

- About vShield Components on page 15

  vShield includes components and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a vSphere Client plug-in, a command line interface (CLI), and REST API.

- Migration of vShield Components on page 17

  The vShield Manager and vShield Edge virtual appliances can be automatically or manually migrated based on DRS and HA policies. The vShield Manager must always be up, so you must migrate the vShield Manager whenever the current ESX host undergoes a reboot or maintenance mode routine.

- About VMware Tools on vShield Components on page 17

  Each vShield virtual appliance includes VMware Tools. Do not upgrade or uninstall the version of VMware Tools included with a vShield virtual appliance.

- Ports Required for vShield Communication on page 17

About vShield Components

vShield includes components and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a vSphere Client plug-in, a command line interface (CLI), and REST API.

To run vShield, you need one vShield Manager virtual machine and at least one vShield App or vShield Edge module.

vShield Manager

The vShield Manager is the centralized network management component of vShield and is installed from OVA as a virtual machine by using the vSphere Client. Using the vShield Manager user interface, administrators install, configure, and maintain vShield components. A vShield Manager can run on a different ESX host from your vShield App and vShield Edge modules.

The vShield Manager leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel.

For more on the using the vShield Manager user interface, see Chapter 2, "vShield Manager User Interface Basics," on page 19.

vShield Edge

vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS port group, or Cisco® Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

NOTE You must obtain an evaluation or full license to use vShield Edge.

Standard vShield Edge Services (Including vCloud Director)

- Firewall: Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for TCP, UDP, and ICMP.
- Network Address Translation: Separate controls for Source and Destination IP addresses, as well as TCP and UDP port translation.
- Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.
- Configuration of DNS servers for relay name resolution requests from clients and syslog servers.
- Static route for data packets to follow.

Advanced vShield Edge Services

- Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocol settings to interoperate with all major firewall vendors.
- Load Balancing: Simple and dynamically configurable virtual IP addresses and server groups.
- High Availability: Ensures that a vShield Edge appliance is always available on your virtualized network.
- SSL VPN-Plus: Allows remote users to connect securely to private networks behind a vShield Edge gateway.

vShield Edge supports syslog export for all services to remote servers.

vShield App

vShield App is an interior, vNIC-level Layer 2 firewall that allows you to create access control policies regardless of network topology and to achieve network isolation in the same VLAN. A vShield App monitors all traffic in and out of an ESX host, including between virtual machines in the same port group. vShield App includes traffic analysis and container-based policy creation. Containers can be dynamic or static, vCenter constructs such as datacenters or objects defined in vShield Manager such as a security group, IPset, or MACset. vShield App supports multi-tenancy.

vShield App installs as a hypervisor module and firewall service virtual appliance. vShield App integrates with ESX hosts through VMsafe APIs and works with VMware vSphere platform features such as DRS, vMotion, DPM, and maintenance mode.

vShield App provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter. Rules can include multiple sources, destinations, and applications. The firewall filter operates transparently and does not require network changes or modification of IP addresses to create security zones. You can write access rules by using vCenter containers, like datacenters, cluster, resource pools and vApps, or network objects, like Port Groups and VLANs, to reduce the number of firewall rules and make the rules easier to track.

You should install vShield App instances on all ESX hosts within a cluster so that VMware vMotion™ operations work and virtual machines remain protected as they migrate between ESX hosts. By default, a vShield App virtual appliance cannot be moved by using vMotion.

The Flow Monitoring feature displays allowed and blocked network flows at the application protocol level. You can use this information to audit network traffic and troubleshoot operational issues.

NOTE You must obtain an evaluation or full license to use vShield App.

vShield Endpoint

vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

vShield Endpoint installs as a hypervisor module and security virtual appliance from a third-party antivirus vendor (VMware partners) on an ESX host.

NOTE You must obtain an evaluation or full license to use vShield Endpoint.

vShield Data Security

vShield Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by vShield Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

Migration of vShield Components

The vShield Manager and vShield Edge virtual appliances can be automatically or manually migrated based on DRS and HA policies. The vShield Manager must always be up, so you must migrate the vShield Manager whenever the current ESX host undergoes a reboot or maintenance mode routine.

Each vShield Edge should move with its datacenter to maintain security settings and services.

vShield App, vShield Endpoint partner appliance, or vShield Data Security cannot be moved to another ESX host. If the ESX host on which these components reside requires a manual maintenance mode operation, you must de-select the **Move powered off and suspended virtual machines to other hosts in the cluster** check box to ensure these virtual appliances are not migrated. These services restart after the ESX host comes online.

About VMware Tools on vShield Components

Each vShield virtual appliance includes VMware Tools. Do not upgrade or uninstall the version of VMware Tools included with a vShield virtual appliance.

Ports Required for vShield Communication

vShield requires the following ports to be open:

- vShield Manager port 443 from the ESX host, the vCenter Server, and the vShield appliances to be deployed
- UDP123 between vShield Manager and vShield App for time synchronization
- 902/TCP and 903/TCP to and from the vCenter Client and ESX hosts
- 443/TCP from the REST client to vShield Manager for using REST API calls

- 80/TCP to 443/TCP for using the vShield Manager user interface and initiating connection to the vSphere SDK
- 22/TCP for troubleshooting the CLI

vShield Manager User Interface Basics

2

The vShield Manager user interface offers configuration and data viewing options specific to vShield use. By utilizing the VMware Infrastructure SDK, the vShield Manager displays your vSphere Client inventory panel for a complete view of your vCenter environment.

NOTE You can register the vShield Manager as a vSphere Client plug-in. This allows you to configure vShield components from within the vSphere Client. See Set up vShield Manager in the *vShield Installation and Upgrade Guide*.

- Log in to the vShield Manager User Interface on page 19

  You access the vShield Manager management interface by using a Web browser.

- About the vShield Manager User Interface on page 20

  The vShield Manager user interface is divided into two panels: the inventory panel and the configuration panel. You select a view and a resource from the inventory panel to open the available details and configuration options in the configuration panel.

Log in to the vShield Manager User Interface

You access the vShield Manager management interface by using a Web browser.

Procedure

1 Open a Web browser window and type the IP address assigned to the vShield Manager.

The vShield Manager user interface opens in an SSL/HTTPS session (or opens a secure SSL session).

2 Accept the security certificate.

NOTE It is recommended that you use an SSL certificate for verification of the vShield Manager. See "Add an SSL Certificate to Identify the vShield Manager Web Service," on page 26.

The vShield Manager login screen appears.

3 Log in to the vShield Manager user interface by using the username **`admin`** and the password **`default`**.

You should change the default password as one of your first tasks to prevent unauthorized use. See "Edit a User Account," on page 41.

4 Click **Log In**.

About the vShield Manager User Interface

The vShield Manager user interface is divided into two panels: the inventory panel and the configuration panel. You select a view and a resource from the inventory panel to open the available details and configuration options in the configuration panel.

When clicked, each inventory object has a specific set of tabs that appear in the configuration panel.

- vShield Manager Inventory Panel on page 20

  The vShield Manager inventory panel hierarchy mimics the vSphere Client inventory hierarchy.

- vShield Manager Configuration Panel on page 21

  The vShield Manager configuration panel presents the settings that can be configured based on the selected inventory resource and the output of vShield operation. Each resource offers multiple tabs, each tab presenting information or configuration forms corresponding to the resource.

vShield Manager Inventory Panel

The vShield Manager inventory panel hierarchy mimics the vSphere Client inventory hierarchy.

Resources include the root folder, datacenters, clusters, port groups, ESX hosts, and virtual machines. As a result, the vShield Manager maintains solidarity with your vCenter Server inventory to present a complete view of your virtual deployment. The vShield Manager and vShield App virtual machines do not appear in the vShield Manager inventory panel. vShield Manager settings are configured from the **Settings & Reports** resource atop the inventory panel.

The inventory panel offers multiple views: Hosts & Clusters, Networks, and Edges. The Hosts & Clusters view displays the datacenters, clusters, resource pools, and ESX hosts in your inventory. The Networks view displays the VLAN networks and port groups in your inventory. The Edges view displays the port groups protected by vShield Edge instances. The Hosts & Clusters and Networks views are consistent with the same views in the vSphere Client.

There are differences in the icons for virtual machines and vShield components between the vShield Manager and the vSphere Client inventory panels. Custom icons are used to show the difference between vShield components and virtual machines, and the difference between protected and unprotected virtual machines.

Table 2-1. vShield Virtual Machine Icons in the vShield Manager Inventory Panel

Icon	Description
	A powered on virtual machine that is protected by a vShield App.
	A powered on virtual machine that is not protected by a vShield App.
	A powered off virtual machine.
	A protected virtual machine that is disconnected.

Refreshing the Inventory Panel

To refresh the list of resources in the inventory panel, click . The refresh action requests the latest resource information from the vCenter Server. By default, the vShield Manager requests resource information from the vCenter Server every five minutes.

Searching the Inventory Panel

To search the inventory panel for a specific resource, type a string in the field atop the vShield Manager inventory panel and click .

vShield Manager Configuration Panel

The vShield Manager configuration panel presents the settings that can be configured based on the selected inventory resource and the output of vShield operation. Each resource offers multiple tabs, each tab presenting information or configuration forms corresponding to the resource.

Because each resource has a different purpose, some tabs are specific to certain resources. Also, some tabs have a second level of options.

Management System Settings 3

You can edit the vCenter Server, DNS and NTP server, and Lookup server that you specified during initial login. The vShield Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

This chapter includes the following topics:

- "Edit DNS Servers," on page 23
- "Edit the vShield Manager Date and Time," on page 24
- "Edit Lookup Service Details," on page 24
- "Edit vCenter Server," on page 24
- "Specify Syslog Server," on page 25
- "Download Technical Support Logs for vShield," on page 25
- "Add an SSL Certificate to Identify the vShield Manager Web Service," on page 26
- "Working with Services and Service Groups," on page 27
- "Grouping Objects," on page 30

Edit DNS Servers

You can change the DNS servers specified during initial login. The primary DNS server appears in the vShield Manager user interface.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Ensure that you are in the **General** tab.

4 Click **Edit** next to **DNS Servers**.

5 Make the appropriate changes.

6 Click **OK**.

Edit the vShield Manager Date and Time

You can change the NTP server specified during initial login.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Ensure that you are in the **General** tab.

4 Click **Edit** next to **NTP Server**.

5 Make the appropriate changes.

6 Click **OK**.

7 Reboot the vShield Manager.

Edit Lookup Service Details

You can change the Lookup Service details specified during initial login.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Ensure that you are in the **General** tab.

4 Click **Edit** next to **Lookup Service**.

5 Make the appropriate changes.

6 Click **OK**.

Edit vCenter Server

You can change the vCenter Server with which you registered vShield Manager upon initial login. You should do this only if you change the IP address of your current vCenter Server.

Procedure

1 If you are logged in to the vSphere Client, log out.

2 Log in to the vShield Manager.

3 Click **Settings & Reports** from the vShield Manager inventory panel.

4 Click the **Configuration** tab.

5 Ensure that you are in the **General** tab.

6 Click **Edit** next to **vCenter Server**.

7 Make the appropriate changes.

8 Click **OK**.

9 Log in to the vSphere Client.

10 Select an ESX host.

11 Verify that **vShield** appears as a tab.

What to do next

You can install and configure vShield components from the vSphere Client.

Specify Syslog Server

If you specify a syslog server, vShield Manager sends all audit logs and system events from vShield Manager to the syslog server.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Ensure that you are in the **General** tab.

4 Click **Edit** next to **Syslog Server**.

5 Type the IP address of the syslog server.

6 (Optional) Type the port for the syslog server.

If you do not specify a port, the default UDP port for the IP address/host name of the syslog server is used.

7 Click **OK**.

Download Technical Support Logs for vShield

You can download vShield Manager audit logs and system events from a vShield component to your PC.

Audit logs refer to configuration change (such as firewall configuration change) logs while system events refer to events that happen in the background while vShield Manager is running. For example, if vShield Manager looses connectivity to one of the vShield App or vShield Edge appliances, a system event is logged.

Both audit logs and system events are logged with the syslog server at the `Info` level. System events, however, have an internal severity which is added to the syslog message sent for that system event.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **Support**.

4 Under **Tech Support Log Download**, click **Initiate** next to the appropriate component.

Once initiated, the log is generated and uploaded to the vShield Manager. This might take several seconds.

5 After the log is ready, click the **Download** link to download the log to your PC.

The log is compressed and has the file extension `.gz`.

What to do next

You can open the log using a decompression utility by browsing for **All Files** in the directory where you saved the file.

Add an SSL Certificate to Identify the vShield Manager Web Service

You can generate a certificate signing request, get it signed by a CA, and import the signed SSL certificate into vShield Manager to authenticate the identity of the vShield Manager web service and encrypt information sent to the vShield Manager web server. As a security best practice, you should use the generate certificate option to generate a private key and public key, where the private key is saved to the vShield Manager.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **SSL Certificate**.

4 Under **Generate Certificate Signing Request**, complete the form by filling in the following fields:

Option	Action
Common Name	Type the IP address or fully qualified domain name (FQDN) of the vShield Manager. VMware recommends that you enter the FQDN.
Organization Unit	Enter the department in your company that is ordering the certificate.
Organization Name	Enter the full legal name of your company.
City Name	Enter the full name of the city in which your company resides.
State Name	Enter the full name of the state in which your company resides.
Country Code	Enter the two-digit code that represents your country. For example, the United States is **US**.
Key Algorithm	Select the cryptographic algorithm to use from either DSA or RSA. VMware recommends RSA for backward compatibility.
Key Size	Select the number of bits used in the selected algorithm.

5 Click **Generate**.

Import an SSL certificate

You can import a pre-existing or CA signed SSL certificate for use by the vShield Manager.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **SSL Certificate**.

4 Under Import Signed Certificate, click **Browse** at Certificate File to find the file.

5 Select the type of certificate file from the **Certificate Type** drop-down list.

If applicable, import root and intermediate certificates before importing the CA signed certificate. If there are multiple intermediate certificates, combine them into a single file and then import the file.

6 Click **Apply**.

A yellow bar containing the message **Successfully imported certificate** is displayed at the top of the screen.

7 Click **Apply Certificate**.

vShield Manager is restarted to apply the certificate.

The certificate is stored in the vShield Manager.

Working with Services and Service Groups

A service is a protocol-port combination, and a service group is a group of services.

Create a Service

You can create a service and then define rules for that service.

Procedure

1 Do one of the following.

Option	Description
To create a service at the global scope	a Log in to the vShield Manager user interface. b Click **Settings & Reports**. c Click **Object Library**.
To create a service at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter from the inventory panel. c Click the **vShield** tab.
To create a service at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To create a service at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Services** tab.

3 Select **Add > Service**.

4 Type a **Name** to identify the service.

5 Type a **Description** for the service.

6 Select a **Protocol** to which you want to add a non-standard port.

7 Type the port number(s) in **Ports**.

8 (Optional) When creating a service at the global or datacenter scope, select **Enable inheritance to allow visibility at underlying scopes** to make this service available to underlying scopes.

9 Click **OK**.

The service appears in the Services table.

Create a Service Group

You can create a service group at the global, datacenter, or vShield Edge level and then define rules for that service group.

Procedure

1 Do one of the following.

Option	Description
To create a service group at the global scope	a Log in to the vShield Manager user interface. b Click **Settings & Reports**. c Click **Object Library**.
To create a service group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab.
To create a service at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To create a service group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Services** tab.

3 Select **Add > Service Group**.

4 Type a **Name** to identify the service group.

5 Type a **Description** for the service.

6 In Members, select the services or service groups that you want to the group.

7 (Optional) When creating a service group at the global or datacenter scope, select **Enable inheritance to allow visibility at underlying scopes** to make this service group available to underlying scopes.

8 Click **OK**.

The custom service group appears in the Services table.

Edit a Service or Service Group

You can edit services and service groups.

A service or service group can be edited at the scope it was defined at. For example, if a service was defined at the global scope, it cannot be edited at the vShield Edge scope.

Procedure

1 Do one of the following.

Option	Description
To edit a service at the global scope	a Log in to the vShield Manager user interface. b Click **Settings & Reports**. c Click **Object Library**.
To edit a service at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab.
To edit a service at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To edit a service at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Services** tab.

3 Select a custom service or service group and click the **Edit** ( ) icon.

4 Make the appropriate changes.

5 Click **OK**.

Delete a Service or Service Group

You can delete services or service group.

A service or service group can be deleted at the scope it was defined at. For example, if a service was defined at the global scope, it cannot be deleted at the vShield Edge scope.

Procedure

1 Do one of the following.

Option	Description
To delete a service at the global scope	a Log in to the vShield Manager user interface. b Click **Settings & Reports**. c Click **Object Library**.
To delete a service at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab.
To delete a service at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To delete a service at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Services** tab.

3 Select a custom service or service group and click the **Delete** ( ) icon.

4 Click **Yes**.

The service or service group is deleted.

Grouping Objects

The Grouping feature enables you to create custom containers to which you can assign resources, such as virtual machines and network adapters, for App Firewall protection. After a group is defined, you can add the group as source or destination to a firewall rule for protection.

Working with IP Address Groups

Create an IP Address Group

You can create an IP address group at the global, datacenter, or vShield Edge scope and then add this group as the source or destination in a firewall rule. Such a rule can help protect physical machines from virtual machines or vice versa.

Procedure

1 Do one of the following.

Option	Description
To create an IP address group at the global scope	a In the vShield Manager user interface, click **Object Library** from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To create an IP address group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.
To create an IP address group at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To create an IP address group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Grouping Objects** tab.

3 Click the **Add** ( ) icon and select **IP Addresses**.

The Add IP Addresses window opens.

4 Type a name for the address group.

5 (Optional) Type a description for the address group.

6 Type the IP addresses to be included in the group.

7 (Optional) When creating an IP address group at the global or datacenter scope, select **Enable inheritance to allow visibility at underlying scopes** to make this IP address group available to underlying scopes.

8 Click **OK**.

Edit an IP Address Group

An IP address group can be edited at the scope it was defined at. For example, if an IP address group was defined at the global scope, it cannot be edited at the vShield Edge scope.

Prerequisites

Procedure

1 Do one of the following.

Option	Description
To edit an IP address group at the global scope	a In the vShield Manager user interface, click **Object Library** from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To edit an IP address group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.
To edit an IP address group at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To edit an IP address group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Grouping Objects** tab.

3 Select the group that you want to edit and click the **Edit** ( ) icon.

4 In the Edit IP Addresses dialog box, make the appropriate changes.

5 Click **OK**.

Delete an IP Address Group

An IP address group can be deleted at the scope it was defined at. For example, if an IP address group was defined at the global scope, it cannot be deleted at the vShield Edge scope.

Procedure

1 Do one of the following.

Option	Description
To delete an IP address group at the global scope	a In the vShield Manager user interface, click **Object Library** from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To delete an IP address group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.

Option	Description
To delete an IP address group at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To delete an IP address group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Grouping Objects** tab.

3 Select the group that you want to delete and click the **Delete** ( ) icon.

Working with MAC Address Groups

Create a MAC Address Group

You can create a MAC address group consisting of a range of MAC addresses and then add this group as the source or destination in a vShield App firewall rule. Such a rule can help protect physical machines from virtual machines or vice versa.

Procedure

1 Do one of the following.

Option	Description
To create a MAC address group at the global level	a In the vShield Manager user interface, click Object Library from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To create a MAC address group at the datacenter level	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.
To create a MAC address at the port group level	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.

2 Click the **Add** ( ) icon and select **MAC Addresses**.

The Add MAC Addresses window opens.

3 Type a name for the address group.

4 (Optional) Type a description for the address group.

5 Type the MAC addresses to be included in the group.

6 Select **Enable inheritance to allow visibility at underlying scopes** if you want the MAC address group to propagate down to objects in the selected datacenter.

7 Click **OK**.

Edit a MAC Address Group

A MAC address group can be edited at the scope it was defined at. For example, if a MAC address group was defined at the global scope, it cannot be edited at the vShield Edge scope.

Procedure

1 Do one of the following.

Option	Description
To edit a MAC address group at the global scope	a In the vShield Manager user interface, click **Object Library** from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To edit a MAC address group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.
To edit a MAC address group at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To edit a MAC address group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Grouping Objects** tab.

3 Select the group that you want to edit and click the **Edit** ( ) icon.

4 In the Edit MAC Addresses dialog box, make the appropriate changes.

5 Click **OK**.

Delete a MAC Address Group

A MAC address group can be deleted at the scope it was defined at. For example, if a MAC address group was defined at the global scope, it cannot be deleted at the vShield Edge scope.

Procedure

1 Do one of the following.

Option	Description
To delete a MAC address group at the global scope	a In the vShield Manager user interface, click **Object Library** from the vShield Manager inventory panel. b Ensure that you are in the **Grouping** tab.
To delete a MAC address group at the datacenter scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d From the General tab, select the **Grouping** tab.

Option	Description
To delete a MAC address group at the port group scope	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab.
To delete a MAC address group at the vShield Edge scope	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **Network Virtualization** tab. d Click the **Edges** tab. e Double-click a vShield Edge instance. f Click the **Configure** tab.

2 Click the **Grouping Objects** tab.

3 Select the group that you want to edit and click the **Delete** ( ) icon.

Working with Security Groups

Create a security group

In the vSphere Client, you can add a security group at the datacenter or port group level.

The security group scope is limited to the resource level at which it is created. For example, if you create a security group at a datacenter level, the security group is available to be added as a source or destination only when you create a firewall rule at the datacenter level. If you create a rule for a port group within that datacenter, the security group is not available.

Procedure

1 Do one of the following.

Option	Description
To create a security group at the datacenter level	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d In the General tab, select the **Grouping** tab.
To create a security group at the port group level	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab. d Select the **Grouping** tab.

2 Click **Add** and select **Security Group**.

The Add Security Group window opens with the selected datacenter displayed as the **Scope**.

3 Type a name and description for the security group.

4 Click in the field next to the Add button and select the resource you want to include in the security group.

5 In **Members**, select one or more resource to add to the security group.

When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

6 Click **OK**.

Edit a Security Group

A security group can be edited at the scope it was defined at. For example, if a security group was defined at the datacenter scope, it cannot be edited at the port group scope.

Procedure

1 Do one of the following.

Option	Description
To edit a security group at the datacenter level	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d In the General tab, select the **Grouping** tab.
To edit a security group at the port group level	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab. d Select the **Grouping** tab.

2 Select the group that you want to edit and click the **Edit** ( ) icon.

3 In the Edit Security Group dialog box, make the appropriate changes.

4 Click **OK**.

Delete a Security Group

A security group can be deleted at the scope it was defined at. For example, if a security group was defined at the datacenter scope, it cannot be deleted at the vShield port group scope.

Procedure

1 Do one of the following.

Option	Description
To delete a security group at the datacenter level	a In the vSphere Client, go to **Inventory > Hosts & Clusters**. b Select a datacenter resource from the inventory panel. c Click the **vShield** tab. d In the General tab, select the **Grouping** tab.
To delete a security group at the port group level	a In the vSphere Client, go to **Inventory > Networking**. b Select a network from the inventory panel. c Click the **vShield** tab. d Select the **Grouping** tab.

2 Select the group that you want to delete and click the **Delete** ( ) icon.

User Management

4

Security operations are often managed by multiple individuals. Management of the overall system is delegated to different personnel according to some logical categorization. However, permission to carry out tasks is limited only to users with appropriate rights to specific resources. From the Users section, you can delegate such resource management to users by granting applicable rights.

vShield supports Single Sign On (SSO), which enables vShield to authenticate users from other identity services such as AD, NIS, and LDAP.

User management in the vShield Manager user interface is separate from user management in the CLI of any vShield component.

This chapter includes the following topics:

- "Configure Single Sign On," on page 37
- "Managing User Rights," on page 38
- "Managing the Default User Account," on page 39
- "Add a User Account," on page 39
- "Edit a User Account," on page 41
- "Change a User Role," on page 41
- "Disable or Enable a User Account," on page 42
- "Delete a User Account," on page 42

Configure Single Sign On

Integrating the single sign on service with vShield improves the security of user authentication for vCenter users and enables vShield to authenticate users from other identity services such as AD, NIS, and LDAP.

With single sign on, vShield supports authentication using authenticated SAML tokens from a trusted source via REST API calls. vShield Manager can also acquire authentication SAML tokens for use with other VMware solutions.

Prerequisites

- Single sign on service must be installed on the vCenter Server.
- NTP server must be specified so that the Single Sign On server time and vShield Manager time is in sync. See Setup vShield Manager in the *vShield Installation and Upgrade Guide*.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Ensure that you are in the **General** tab.

4 Click **Edit** next to **Lookup Service**.

5 Type the name or IP address of the host that has the lookup service.

6 Change the port number if required.

The Lookup Service URL is displayed based on the specified host and port.

7 Type the SSO user name and password.

This enables vShield Manager to register itself with the Security Token Service server.

8 Click **OK**.

What to do next

Assign a role to the SSO user.

Managing User Rights

Within the vShield Manager user interface, a user's role define the actions the user is allowed to perform on a given resource. The role determine the user's authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows domain control over specific resources, or system-wide control if your right has no restrictions.

The following rules are enforced:

- A user can only have one role.
- You cannot add a role to a user, or remove an assigned role from a user. You can, however, change the assigned role for a user.

Table 4-1. vShield Manager User Roles

Right	Permissions
Enterprise Administrator	vShield operations and security.
vShield Administrator	vShield operations only: for example, install virtual appliances, configure port groups.
Security Administrator	vShield security only: for example, define data security policies, create port groups, create reports for vShield modules.
Auditor	Read only.

The scope of a role determines what resources a particular user can view. The following scopes are available for vShield users.

Table 4-2. vShield Manager User Scope

Scope	Description
No restriction	Access to entire vShield system
Limit access scope to the selected port groups below	Access to a specified datacenter or port group

The Enterprise Administrator and vShield Administrator roles can only be assigned to vCenter users, and their access scope is global (no restrictions).

Managing the Default User Account

The vShield Manager user interface includes a local user account, which has access rights to all resources. You cannot edit the rights of or delete this user. The default user name is **admin** and the default password is **default**.

Change the password for this account upon initial login to the vShield Manager. See "Edit a User Account," on page 41.

Add a User Account

You can either create a new user local to vShield, or assign a role to a vCenter user.

Create a New Local User

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Click **Add**.

The Assign Role window opens.

4 Click **Create a new user local to vShield**.

5 Type an **Email** address.

6 Type a **Login ID**.

This is used for login to the vShield Manager user interface. This user name and associated password cannot be used to access the vShield App or vShield Manager CLIs.

7 Type the user's **Full Name** for identification purposes.

8 Type a **Password** for login.

9 Re-type the password in the **Retype Password** field.

10 Click **Next**.

11 Select the role for the user and click **Next**. For more information on the available roles, see "Managing User Rights," on page 38.

12 Select the scope for the user and click **Finish**.

The user account appears in the Users table.

Assign a Role to a vCenter User

When you assign a role to an SSO user, vCenter authenticates the user with the identity service configured on the SSO server. If the SSO server is not configured or is not available, the user is authenticated either locally or with Active Directory based on vCenter configuration.

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Click **Add**.

The Assign Role window opens.

4 Click **Select vCenter user**.

5 Type the vCenter **User** name for the user.

NOTE If the vCenter user is from a domain (such as a SSO user), then you must enter a fully qualified windows domain path. This will allow the default vShield Manager user (admin) as well as the SSO default user (admin) to login to vShield Manager. This user name is for login to the vShield Manager user interface, and cannot be used to access the vShield App or vShield Manager CLIs.

6 Click **Next**.

7 Select the role for the user and click **Next**. For more information on the available roles, see "Managing User Rights," on page 38.

8 Select the scope for the user and click **Finish**.

The user account appears in the Users table.

Understanding Group Based Role Assignments

Organizations create user groups for proper user management. After integration with Single Sign On (SSO), vShield Manager can get the details of groups to which a user belongs to. Instead of assigning roles to individual users who may belong to the same group, vShield Manager assigns roles to groups. Let us walk through some scenarios to help us understand how vShield Manager assigns roles.

Example: Scenario 1

Group option	Value
Name	G1
Role assigned	Auditor (Read only)
Resources	Global root

User option	Value
Name	John
Belongs to group	G1
Role assigned	None

John belongs to group G1 which has been assigned the auditor role. John inherits the group role and resource permissions.

Example: Scenario 2

Group option	Value
Name	G1
Role assigned	Auditor (Read only)
Resources	Global root

Group option	Value
Name	G2
Role assigned	Security Administrator (Read and Write)
Resources	Datacenter1

User option	Value
Name	Joseph
Belongs to group	G1, G2
Role assigned	None

Joseph belongs to groups G1 and G2 and inherits a combination of the rights and permissions of the Auditor and Security Administrator roles. For example, John has the following permissions:

- Read, write (Security Administrator role) for Datacenter1
- Read only (Auditor) for global root

Example: Scenario 3

Group option	Value
Name	G1
Role assigned	Enterprise Administrator
Resources	Global root

User option	Value
Name	Bob
Belongs to group	G1
Role assigned	Security Administrator (Read and Write)
Resources	Datacenter1

Bob has been assigned the Security Administrator role, so he does not inherit the group role permissions. Bob has the following permissions

- Read, write (Security Administrator role) for Datacenter1 and its child resources
- Enterprise Administrator role on Datacenter1

Edit a User Account

You can edit a user account to change the role or scope. You cannot edit the **`admin`** account.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Select the user you want to edit.

4 Click **Edit**.

5 Make changes as necessary.

6 Click **Finish** to save your changes.

Change a User Role

You can change the role assignment for all users, except for the **`admin`** user.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Select the user you want to change the role for

4 Click **Change Role**.

5 Make changes as necessary.

6 Click **Finish** to save your changes.

Disable or Enable a User Account

You can disable a user account to prevent that user from logging in to the vShield Manager. You cannot disable the **admin** user.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Select a user account.

4 Do one of the following.

- Click **Actions > Disable selected user(s)** to disable a user account.
- Click **Actions > Enable selected user(s)** to enable a user account.

Delete a User Account

You can delete any created user account. You cannot delete the **admin** account. Audit records for deleted users are maintained in the database and can be referenced in an Audit Log report.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Users** tab.

3 Select the user you want to delete.

4 Click **Delete**.

5 Click **OK** to confirm deletion.

If you delete a vCenter user account, only the role assignment for vShield Manager is deleted. The user account on vCenter is not deleted.

Updating System Software 5

vShield software requires periodic updates to maintain system performance. Using the **Updates** tab options, you can install and track system updates.

- View the Current System Software on page 43

  You can view the current installed versions of vShield component software or verify if an update is in progress.

- Upload an Update on page 43

  vShield updates are available as offline updates. When an update is made available, you can download the update to your PC, and then upload the update by using the vShield Manager user interface.

View the Current System Software

You can view the current installed versions of vShield component software or verify if an update is in progress.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Updates** tab.

3 Click **Update Status**.

Upload an Update

vShield updates are available as offline updates. When an update is made available, you can download the update to your PC, and then upload the update by using the vShield Manager user interface.

When the update is uploaded, the vShield Manager is updated first, after which, each vShield Zones or vShield App instance is updated. If a reboot of either the vShield Manager or a vShield Zones or App is required, the **Update Status** screen prompts you to reboot the component. In the event that both the vShield Manager and all vShield Zones or App instances must be rebooted, you must reboot the vShield Manager first, and then reboot each vShield Zones or App.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Updates** tab.

3 Click **Upload Upgrade Bundle**.

4 Click **Browse** to locate the update.

5 After locating the file, click **Upload File**.

6 Click **Update Status** and then click **Install**.

7 Click **Confirm Install** to confirm update installation.

There are two tables on this screen. During installation, you can view the top table for the description, start time, success state, and process state of the current update. View the bottom table for the update status of each vShield App. All vShield App instances have been upgraded when the status of the last vShield App is displayed as **Finished**.

8 After the vShield Manager reboots, click the **Update Status** tab.

9 Click **Reboot Manager** if prompted.

10 Click **Finish Install** to complete the system update.

11 Click **Confirm**.

Backing Up vShield Manager Data 6

You can back up and restore your vShield Manager data, which can include system configuration, events, and audit log tables. Configuration tables are included in every backup. You can, however, exclude system and audit log events. Backups are saved to a remote location that must be accessible by the vShield Manager.

Backups can be executed according to a schedule or on demand.

- Back Up Your vShield Manager Data on Demand on page 45

  You can back up vShield Manager data at any time by performing an on-demand backup.

- Schedule a Backup of vShield Manager Data on page 46

  You can only schedule the parameters for one type of backup at any given time. You cannot schedule a configuration-only backup and a complete data backup to run simultaneously.

- Restore a Backup on page 46

  You can restore a backup only on a freshly deployed vShield Manager appliance.

Back Up Your vShield Manager Data on Demand

You can back up vShield Manager data at any time by performing an on-demand backup.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **Backups**.

4 (Optional) Select the **Exclude System Events** check box if you do not want to back up system event tables.

5 (Optional) Select the **Exclude Audit Logs** check box if you do not want to back up audit log tables.

6 Type the **Host IP Address** of the system where the backup will be saved.

7 Type the **Host Name** of the backup system.

8 Type the **User Name** required to log in to the backup system.

9 Type the **Password** associated with the user name for the backup system.

10 In the **Backup Directory** field, type the absolute path where backups are to be stored.

11 Type a text string in **Filename Prefix**.

This text is prepended to the backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.

12 Enter a **Pass Phrase** to secure the backup file.

13 From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**.

14 Click **Backup**.

Once complete, the backup appears in a table below this forms.

15 Click **Save Settings** to save the configuration.

Schedule a Backup of vShield Manager Data

You can only schedule the parameters for one type of backup at any given time. You cannot schedule a configuration-only backup and a complete data backup to run simultaneously.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **Backups**.

4 From the **Scheduled Backups** drop-down menu, select **On**.

5 From the **Backup Frequency** drop-down menu, select **Hourly**, **Daily**, or **Weekly**.

The **Day of Week**, **Hour of Day**, and **Minute** drop-down menus are disabled based on the selected frequency. For example, if you select **Daily**, the **Day of Week** drop-down menu is disabled as this field is not applicable to a daily frequency.

6 (Optional) Select the **Exclude System Events** check box if you do not want to back up system event tables.

7 (Optional) Select the **Exclude Audit Log** check box if you do not want to back up audit log tables.

8 Type the **Host IP Address** of the system where the backup will be saved.

9 (Optional) Type the **Host Name** of the backup system.

10 Type the **User Name** required to login to the backup system.

11 Type the **Password** associated with the user name for the backup system.

12 In the **Backup Directory** field, type the absolute path where backups will be stored.

13 Type a text string in **Filename Prefix**.

This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.

14 From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.

15 Click **Save Settings**.

Restore a Backup

You can restore a backup only on a freshly deployed vShield Manager appliance.

To restore an available backup, the **Host IP Address**, **User Name**, **Password**, and **Backup Directory** fields in the **Backups** screen must have values that identify the location of the backup to be restored. If the backup file contains system event and audit log data, that data is also restored.

IMPORTANT Back up your current data before restoring a backup file.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Configuration** tab.

3 Click **Backups**.

4 Click **View Backups** to view all available backups saved to the backup server.

5 Select the check box for the backup to restore.

6 Click **Restore**.

7 Click **OK** to confirm.

7 System Events and Audit Logs

System events are events that are related to vShield operation. They are raised to detail every operational event, such as a vShield App reboot or a break in communication between a vShield App and the vShield Manager. Events might relate to basic operation (Informational) or to a critical error (Critical).

This chapter includes the following topics:

- "View the System Event Report," on page 49
- "vShield Manager Virtual Appliance Events," on page 49
- "vShield App Events," on page 50
- "About the Syslog Format," on page 51
- "View the Audit Log," on page 51

View the System Event Report

The vShield Manager aggregates system events into a report.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **System Events** tab.

3 To sort events, click or next to the appropriate column header.

vShield Manager Virtual Appliance Events

The following events are specific to the vShield Manager virtual appliance.

Table 7-1. vShield Manager Virtual Appliance Events

	Power Off	Power On	Interface Down	Interface Up
Local CLI	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.
GUI	NA	NA	NA	NA

Table 7-2. vShield Manager Virtual Appliance Events

	CPU	Memory	Storage
Local CLI	Run `show process monitor` command.	Run `show system memory` command.	Run `show filesystem` command.
GUI	NA	NA	NA

vShield App Events

The following events are specific to vShield App virtual appliances.

Table 7-3. vShield App Events

	Power Off	Power On	Interface Down	Interface Up
Local CLI	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.	Run `show log follow` command.
Syslog	NA	See "About the Syslog Format," on page 51.	`e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex`. For scripting on the syslog server, search for **`NIC Link is`**.	`e1000: mgmt: e1000_watchdog_task: NIC Link is Up/Down 100 Mbps Full Duplex`. For scripting on the syslog server, search for **`NIC Link is`**.
GUI	"Heartbeat failure" event in System Event log. See "View the System Event Report," on page 49.	See "Viewing the Current System Status of a vShield App," on page 158.	See "Viewing the Current System Status of a vShield App," on page 158.	See "Viewing the Current System Status of a vShield App," on page 158.

Table 7-4. vShield AppAppliance Status Events

	CPU	Memory	Storage	Session reset due to DoS, Inactivity, or Data Timeouts
Local CLI	Run `show process monitor` command.	Run `show system memory` command.	Run `show filesystem` command.	Run `show log follow` command.
Syslog	NA		NA	See "About the Syslog Format," on page 51.
GUI	1 From the vShield Manager inventory panel, select the host which has vShield App installed. 2 In **Service Virtual Machines**, click ▶ next to the vShield App virtual machine.	1 From the vShield Manager inventory panel, select the host which has vShield App installed. 2 In **Service Virtual Machines**, click ▶ next to the vShield App virtual machine.	1 From the vShield Manager inventory panel, select the host which has vShield App installed. 2 In **Service Virtual Machines**, click ▶ next to the vShield App virtual machine.	1 From the vShield Manager inventory panel, select the host which has vShield App installed. 2 In **Service Virtual Machines**, click ▶ next to the vShield App virtual machine.

About the Syslog Format

Is this the same for SPOCK?

The system event message logged in the syslog has the following structure.

```
syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter '::' (double colons)
Each name/value pair separated by delimiter ';;' (double semi-colons)
```

The fields and types of the system event contain the following information.

```
Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (possible values: 10007 10016 10043 20019)
Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::
```

View the Audit Log

The **Audit Logs** tab provides a view into the actions performed by all vShield Manager users. The vShield Manager retains audit log data for one year, after which time the data is discarded.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click the **Audit Logs** tab.

3 To view details of an audit log, click the text in the **Operation** column. When details are available for an audit log, the text in the **Operation** column for that log is clickable.

4 In the **Audit Log Change Details**, select **Changed Rows** to display only properties whose values have changed after the operation was performed.

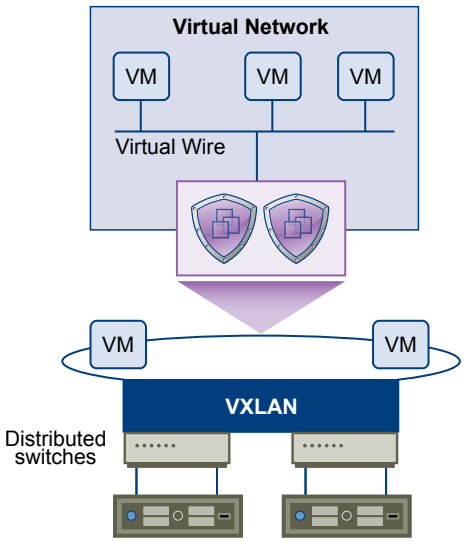
VXLAN Virtual Wires Management

8

In large cloud deployments, applications within virtual networks may need to be logically isolated. For example, a three-tier application can have multiple virtual machines requiring logically isolated networks between the virtual machines. Traditional network isolation techniques such as VLAN (4096 LAN segments through a 12-bit VLAN identifier) may not provide enough segments for such deployments. In addition, VLAN based networks are bound to the physical fabric and their mobility is restricted.

The vShield VXLAN virtual wire is a scalable flat Layer 2 network segment. This feature allows you provides network agility by allowing you to deploy an application on any available cluster and transport virtual machines across a broader diameter. The underlying technology, referred to as Virtual eXtensible LAN (or VXLAN), defines a 24-bit LAN segment identifier to provide segmentation at cloud-deployment scale. VXLAN virtual wires enable you to grow your cloud deployments with repeatable pods in different subnets. Cross cluster placement of virtual machines helps you to fully utilize your network resources without any physical re-wiring. VXLAN virtual wires thus provide application level isolation.

Figure 8-1. VXLAN Virtual wire overview



You must be a Security Administrator in order to create VXLAN virtual wires.

This chapter includes the following topics:

- "Preparing your Network for VXLAN Virtual Wires," on page 54
- "Create a VXLAN Virtual Wire," on page 55
- "Connect Virtual Machines to a VXLAN Virtual Wire," on page 57
- "Test VXLAN Virtual Wire Connectivity," on page 58

- "Viewing Flow Monitoring Data for a VXLAN Virtual Wire," on page 59
- "Working with Firewall Rules for VXLAN Virtual Wires," on page 59
- "Prevent Spoofing on a VXLAN Virtual Wire," on page 60
- "Editing Network Scopes," on page 60
- "Edit a VXLAN Virtual Wire," on page 61
- "Sample Scenario for Creating VXLAN Virtual Wires," on page 62

Preparing your Network for VXLAN Virtual Wires

You must prepare your network for VXLAN virtual wires by specifying a transport VLAN and enabling IP multicast. These preparation steps need to be done only once - you can then create multiple VXLAN virtual wires.

Prerequisites

Go through the following checklist to prepare for creating VXLAN virtual wires in your network:

- Ensure that you have the following software versions
  - VMware vCenter Server 5.1 or later
  - VMware ESX 5.1 or later on each server
  - vSphere Distributed Switch 5.1 or later
- Physical infrastructure MTU must be at least 50 bytes more than the MTU of the virtual machine vNIC
- Get multicast address range from your network administrator and segment ID pool
- Set Managed IP address for each vCenter server in the vCenter Server Runtime Settings. For more information, see vCenter Server and Host Management.
- Verify that DHCP is available on VXLAN transport VLANs
- For Link Aggregation Control Protocol (LACP), 5- tuple hash distribution must be enabled

Associating Clusters with Distributed Switches

You must map each cluster that is to participate in a virtualized network to a vDS. When you map a cluster to a switch, each host in that cluster is enabled for VXLAN virtual wires.

Prerequisites

VMware recommends that you use a consistent switch type (vendor etc.) and version across a given network scope. Inconsistent switch types can lead to undefined behavior in your VXLAN virtual wire.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Ensure that you are in the **Preparation** tab.

5 In Connectivity, click **Edit.**

The **Prepare Infrastructure for VXLAN networking** dialog box appears.

6 Select the clusters that are to participate in the virtual network.

7 For each selected cluster, type the VLAN used for VXLAN transport.

For information on retrieving the VLAN ID of the VXLAN VLAN, see the vSphere Networking documentation.

8 Click **Next**.

9 In Specify Transport Attributes, type the Maximum Transmission Units (MTU) for each virtual distributed switch. MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. VXLAN traffic frames are slightly larger in size because of the encapsulation, so the MTU for each switch must be set to 1550 or higher.

10 Click **Finish**.

You have now pooled your compute resources and are ready to create VXLAN virtual wires on demand.

Assign Segment ID Pool and Multicast Address Range to vShield Manager

You must specify a segment ID pool to isolate your network traffic, and a multicast address range to help in spreading traffic across your network to avoid overloading a single multicast address.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Ensure that you are in the **Preparation** tab.

5 Click the **Segment ID** tab.

6 Click **Edit**.

The Edit Settings dialog box opens.

7 Type a range for segment IDs. For example, **`5000–5200`**.

8 Type an address range. For example, **`224.1.1.50–224.1.1.60`**.

9 Click **OK**.

Create a VXLAN Virtual Wire

Prerequisites

Your network is prepared for VXLAN virtual wires.

Add a Network Scope

A network scope is the compute diameter spanned by your virtualized network and may contain multiple VXLAN virtual wires.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Network Scopes** tab.

5 Click the **Add** ( ) icon.

The Add Network Scope dialog box opens.

6 Type a name for the network scope.

7 Type a description for the network scope.

8 Select the clusters you want to add to the network scope.

9 Click **OK**.

Add a VXLAN Virtual Wire

After you prepare the VXLAN fabric, you can add a VXLAN virtual wire. A VXLAN virtual wire provides the necessary networking abstraction so that the vNICs of a virtual machine always use a VXLAN virtual wire for connectivity to outside world.

Prerequisites

1 Your network is prepared for VXLAN virtual wires.

2 You have added a network scope.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 Click the **Add** icon.

6 Type a name for the VXLAN virtual wire.

7 Type a description for the VXLAN virtual wire.

8 Select the network scope in which you want to create the virtualized network. The Scope Details panel displays the clusters that are part of the selected network scope and the services available to be deployed on the scope.

9 Click **OK**.

What to do next

Click on the VXLAN virtual wire in the Name column to view the virtual wire details.

Connect a VXLAN Virtual Wire to a vShield Edge

Connecting a VXLAN virtual wire to a vShield Edge interface to isolates the VXLAN virtual wire and provides network edge security.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 Select the VXLAN virtual wire that you want to connect a vShield Edge.

6 Click the **More Actions** ( ) icon and select **Connect to Edge**.

7 Select the vShield Edge to which you want to connect the VXLAN virtual wire.

8 Click **Select**.

9 In the Redirect to Selected Edge dialog box, click **Continue**.

10 In the Edit Edge Interface dialog box, type a name for the vShield Edge interface.

11 Select **Internal** or **Uplink** to indicate whether this is an internal or uplink interface.

A VXLAN virtual wire is typically connected to an internal interface.

12 The VXLAN virtual wire name is displayed in the **Connected To** area.

13 Select the connectivity status for the interface.

14 If the vShield Edge to which you are connecting the VXLAN virtual wire to has Manual HA Configuration selected, specify two management IP addresses in CIDR format.

15 Edit the default MTU if required.

16 Click **OK**.

Deploy Services on a VXLAN Virtual Wire

You can deploy third party services on a VXLAN virtual wire.

Prerequisites

For information on adding services to vShield Manager, see "Inserting a Network Services," on page 151.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 In the **Name** column, click the virtual wire that you want to deploy services on.

6 In the **Available Services** panel, click **Enable Services**.

7 In the Apply Service Profile to this Network dialog box, select the service and service profile that you want to apply.

8 Click **Apply**.

Connect Virtual Machines to a VXLAN Virtual Wire

You can connect virtual machines to a VXLAN virtual wire. This makes it easy to identify the port groups that belong to a virtual wire in your vCenter inventory.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 In the **Name** column, click the VXLAN virtual wire that you want to edit.

6 Click the **Virtual Machines** tab.

7 Click the **Add** ( ) icon.

8 In the Connect VNics to this Network dialog box, type the name of the virtual machine in the Search field and click .

All VNics for the virtual machine are displayed.

9 Select the VNics that you want to connect.

10 Click **Next**.

11 Review the VNics you selected.

12 Click **Finish**.

Test VXLAN Virtual Wire Connectivity

You can do a ping or broadcast test on a VXLAN virtual wire to check its connectivity and physical infrastructure plumbing for VXLAN.

Perform Ping Test

You can ping a destination host from a source host before sending a unicast packet.

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 In the **Name** column, click the VXLAN virtual wire that you want to test.

6 Click the **Hosts** tab.

7 Select a host.

8 Click the **More Actions** ( ) icon and select **Test Connectivity**.

The Test Connectivity Between Hosts in the Network dialog box opens. The host you selected in step 7 appears in the Source host field. Select **Browse** to select a different source host.

9 Select the size of the test packet.

VXLAN standard size is 1550 bytes (should match the physical infrastructure MTU) without fragmentation. This allows vShield to check connectivity and verify that the infrastructure is prepared for VXLAN traffic.

Minimum packet size allows fragmentation. Hence, vShield can check only connectivity but not whether the infrastructure is ready for the larger frame size.

10 In the **Destination** panel, click **Browse Hosts**.

11 In the Select Host dialog box, select the destination host.

12 Click **Select**.

13 Click **Start Test**.

The host-to-host ping test results are displayed.

Perform Broadcast Test

You can perform a broadcast test to resolve MAC addresses. A single host sends a broadcast message to all other devices on the same network segment.

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 In the **Name** column, click the virtual wire that you want to test.

6 Click the **Hosts** tab.

7 Select a host.

8 Click the **More Actions** ( ) icon and select **Test Connectivity**.

9 In the Test Connectivity Between Hosts in the Network dialog box, click **Broadcast**

The host you selected in step 7 appears in the Source host field. Select **Browse** to select a different source host.

10 Select the size of the test packet.

VXLAN standard size is 1550 bytes (should match the physical infrastructure MTU) without fragmentation. This allows vShield to check connectivity and verify that the infrastructure is prepared for VXLAN traffic.

Minimum packet size allows fragmentation. Hence, vShield can check infrastructure connectivity but not whether the infrastructure is ready for the larger frame size.

11 Click **Start Test**.

The broadcast test results are displayed.

Viewing Flow Monitoring Data for a VXLAN Virtual Wire

Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic on your VXLAN virtual wire that passed through a vShield App. The Flow Monitoring output defines which machines are exchanging data and over which application. This data includes the number of sessions, packets, and bytes transmitted per session. Session details include sources, destinations, direction of sessions, applications, and ports being used. Session details can be used to create firewall allow or block rules.

You can use Flow Monitoring as a forensic tool to detect rogue services and examine outbound sessions. Flow monitoring data is available for two weeks.

Flow monitoring data is available only if you have vShield App installed on the hosts in the VXLAN virtual wire clusters.

For more information, see Chapter 12, “vShield App Flow Monitoring,” on page 161.

Working with Firewall Rules for VXLAN Virtual Wires

vShield App provides firewall protection to your VXLAN virtual wires through access policy enforcement.

For more information, see Chapter 13, “vShield App Firewall Management,” on page 167.

Prevent Spoofing on a VXLAN Virtual Wire

After synchronizing with the vCenter Server, vShield Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. vShield does not trust all IP address provided by VMware Tools on a virtual machine. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

SpoofGuard allows you to authorize the IP addresses reported by VMware Tools, and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from the App Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

For more information, see "Using SpoofGuard," on page 174.

Editing Network Scopes

You can edit, expand, or contract a network scope.

View and Edit a Network Scope

You can view the VXLAN virtual wires in a selected network scope, the clusters in, and the services available for that network scope.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Network Scope** tab.

All network scopes for the selected datacenter are displayed.

5 In the **Name** column, click on a network scope.

The Summary tab displays the following information. Click **Edit** in the appropriate section to make changes.

- The Properties section displays the name and description of the network scope and the number of VXLAN virtual wires based on this network scope.
- The Network Scope section displays the clusters in the network scope and whether they are ready for virtualized networking (i.e. whether the clusters have been mapped to a vDS).
- The Available Services section displays the services available for the network scope.

Expand a Network Scope

You can add clusters to a network scope. This will stretch all existing VXLAN virtual wires to become available on the newly added clusters.

Prerequisites

The clusters you add to a network scope must be prepared. See "Preparing your Network for VXLAN Virtual Wires," on page 54.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Network Scope** tab.

All network scope for the selected datacenter are displayed.

5 In the **Name** column, click a network scope.

6 In **Scope Details**, click **Expand**.

The Add Clusters to a Network Scope (Expand) dialog box opens.

7 Select the clusters you want to add to the network scope.

8 Click **OK**.

Contract a Network Scope

You can remove clusters from a network scope. Existing VXLAN virtual wires may be shrunk to accommodate the contracted scope.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Network Scope** tab.

All network scopes for the selected datacenter are displayed.

5 In the **Name** column, click on a network scope.

6 In **Scope Details**, click **Contract**.

The Remove Clusters from a Network Scope (Contract) dialog box opens.

7 Select the clusters you want to remove from the network scope.

8 Click **OK**.

Edit a VXLAN Virtual Wire

You can edit the name and description of a VXLAN virtual wire.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 In the **Name** column, click the VXLAN virtual wire to edit.

6 Click **Edit**.

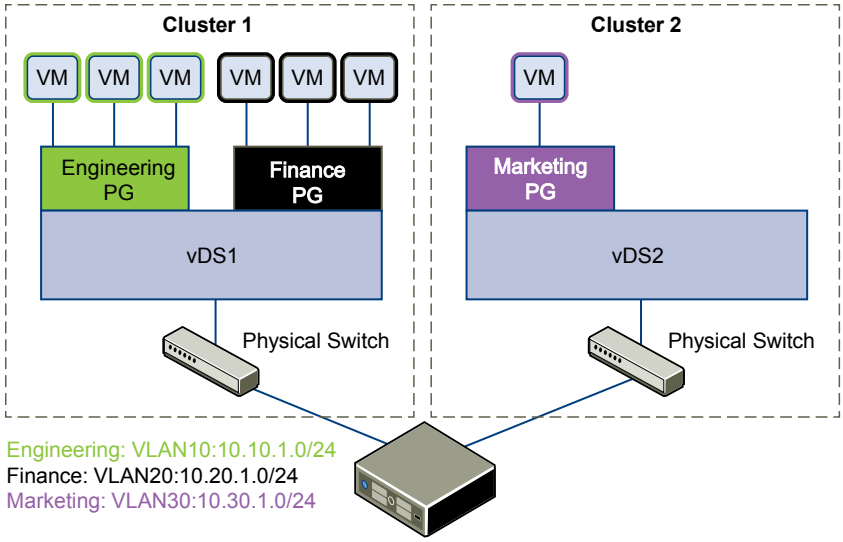
7 Make the desired changes.

8 Click **OK**.

Sample Scenario for Creating VXLAN Virtual Wires

This scenario presents a situation where company ACME Enterprise has several ESX hosts on two clusters in a datacenter, ACME_Datacenter. The Engineering (on port group PG-Engineering) and Finance departments (on port group PG-Finance) are on Cluster1. The Marketing department (PG-Marketing) is on Cluster2. Both clusters are managed by a single vCenter Server 5.1.

Figure 8-2. ACME Enterprise network before implementing VXLAN virtual wires

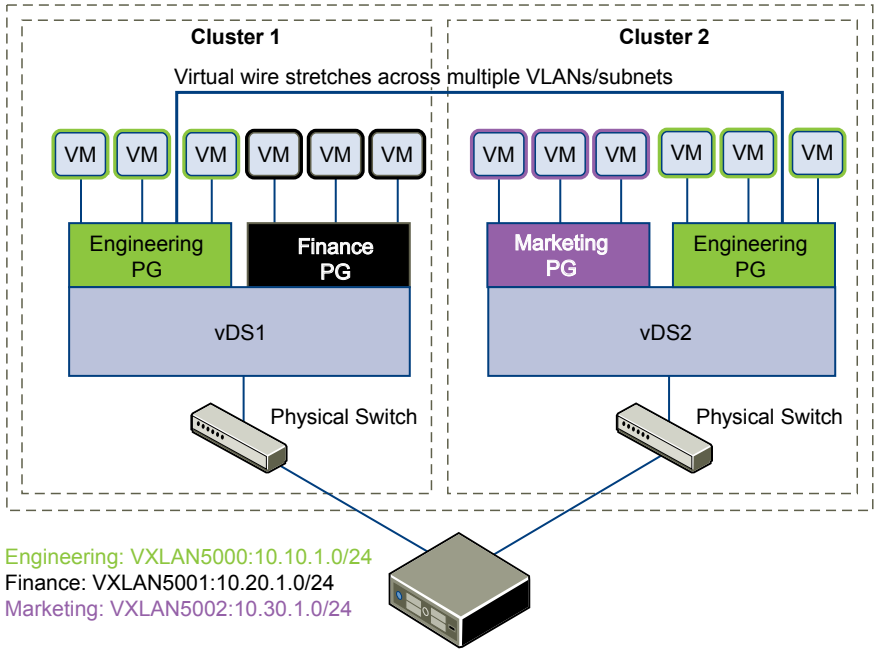


ACME is running out of compute space on Cluster1 while Cluster2 is under-utilized. The ACME network supervisor asks John Admin (ACME's virtualization administrator) to figure out a way to extend the Engineering department to Cluster2 in a way that virtual machines belonging to Engineering on both clusters can communicate with each other. This would enable ACME to utilize the compute capacity of both clusters by stretching ACME's L2 layer.

If John Admin were to do this the traditional way, he would need to connect the separate VLANs in a special way so that the two clusters can be in the same L2 domain. This might require ACME to buy a new physical device to separate traffic, and lead to issues such as VLAN sprawl, network loops, and administration and management overhead.

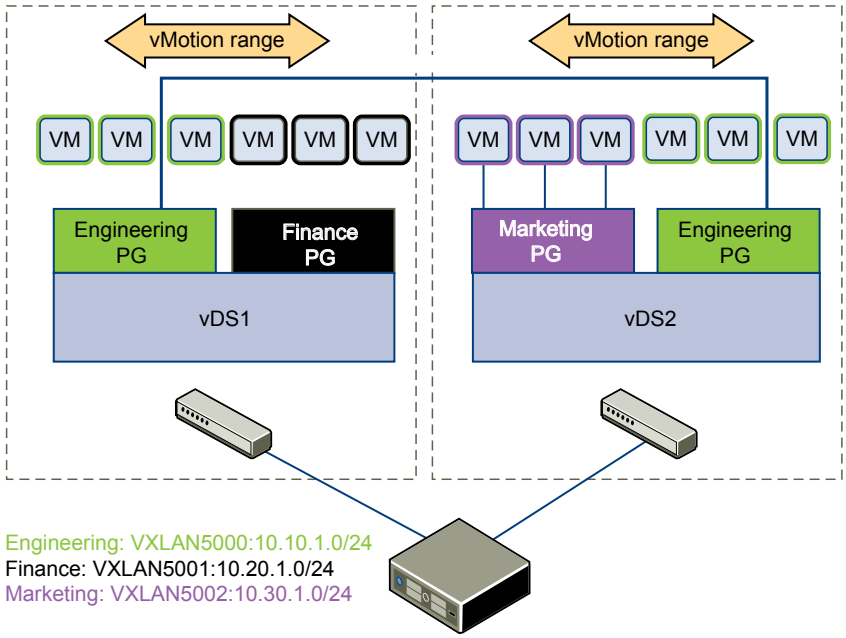
John Admin remembers seeing a VXLAN virtual wire demo at VMworld 2011, and decides to evaluate the vShield 5.1 release. He concludes that building a VXLAN virtual wire across dvSwitch1 and dvSwitch2 will allow him to stretch ACME's L2 layer.

Figure 8-3. ACME Enterprise implements a VXLAN virtual wire



Once John Admin builds a VXLAN virtual wire across the two clusters, he can vMotion virtual machines across the VDSes.

Figure 8-4. vMotion on a VXLAN virtual wire



Let us walk through the steps that John Admin follows to build a VXLAN virtual wire at ACME Enterprise.

John Admin Associates Cluster with Distributed Switches

John Admin must map each cluster that is to participate in a virtualized network to a vDS. When he maps a cluster to a switch, each host in that cluster is enabled for VXLAN virtual wires.

Prerequisites

1 John Admin gets a segment ID pool (4097 - 5010) from ACME's vShield manager admin and a multi cast address range (224.0.0.0 to 239.255.255.255) from ACME's network administrator.

2 John Admin sets the Managed IP address for the vCenter Server.

   a Select **Administration > vCenter Server Settings > Runtime Settings**.

   b In vCenter Server Managed IP, type **`10.115.198.165`**.

   c Click **OK**.

3 John Admin ensures that a DHCP server is available on VXLAN transport VLANs.

4 John Admin verifies that both dvSwitch1 and dvSwitch2 are the same version and from the same vendor.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select ACME_Datacenter from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Ensure that you are in the **Preparation** tab.

5 In Connectivity, click **Edit**.

6 In the Prepare Infrastructure for VXLAN networking dialog box, select Cluster1 to participate in the VXLAN virtual wire.

7 Type **`10`** for dvSwitch1 to use as the ACME VXLAN transport VLAN.

8 Click **Next**.

9 In Specify Transport Attributes, leave 1600 as the Maximum Transmission Units (MTU) for dvSwitch1.

   MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. John Admin knows that VXLAN virtual wire traffic frames are slightly larger in size because of the encapsulation, so the MTU for each switch must be set to 1550 or higher.

10 Repeat steps 5 through step 7 and select Cluster2 to participate in the VXLAN virtual wire.

11 In Specify Transport Attributes, type **`20`** for dvSwitch2.

12 Leave 1600 as the Maximum Transmission Units (MTU) for dvSwitch2.

13 Click **Finish**.

After John admin maps Cluster1 and Cluster2 to the appropriate switch, the hosts on those clusters are prepared for VXLAN virtual wires:

1 A VXLAN kernel module and vmknic is added to each host in Cluster1 and Cluster2.

2 A special dvPortGroup is created on the vDS associated with the VXLAN virtual wire and the vmknic is connected to it.

John Admin Assigns Segment ID Pool and Multicast Address Range to vShield Manager

John Admin must specify the segment ID pool he received to isolate Company ABC's network traffic and the multicast address range to help in spreading traffic across the network to avoid overloading a single multicast address.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select ABC_Datacenter from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Ensure that you are in the **Preparation** tab.

5 Click the **Segment ID** tab.

6 Click **Edit**.

The Edit Settings dialog box opens.

7 In Segment ID pool, type **`500–510`**.

8 In Multicast addresses, type **`224.1.1.50–224.1.1.60`**.

9 Click **OK**.

John Admin Adds a Network Scope

The physical network backing a VXLAN virtual wire is called a network scope. A network scope is the compute diameter spanned by a virtualized network.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select ABC_Datacenter from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Network Scopes** tab.

5 Click the **Add** ( ) icon.

The Add Network Scope dialog box opens.

6 In Name, type **ACME Scope**.

7 In Description, type **Scope containing ACME's clusters**.

8 Select Cluster1 and Cluster2 to add to the network scope.

9 Click **OK**.

John Admin Adds a VXLAN Virtual Wire

After John Admin prepares the VXLAN virtual wire fabric, he can add a VXLAN virtual wire. A VXLAN virtual wire provides the necessary networking abstraction so that the vNICs of a VXLAN virtual wire always use a VXLAN virtual wire for connectivity to outside world.

Prerequisites

1 ACME's network is prepared for VXLAN virtual wires.

2 John Admin has added a network scope.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select ABC_Datacenter from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Networks** tab.

5 Click the **Add** icon.

6 In Name, type **`ACME virtual wire`**.

7 In Description, type **`Virtual wire for extending ACME Engineering network to Cluster2`**.

8 In **Network Scope**, select ACME Scope.

9 Review the Scope Details.

10 Click **OK**.

vShield creates a VXLAN virtual wire providing L2 connectivity (via VXLANs) between dvSwitch1 and dvSwitch2.

What to do next

John Admin can now connect ACME's production virtual machines to the VXLAN virtual wire, and connect the VXLAN virtual wire to a vShield Edge.

vShield Edge Management

9

vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, vDS port group, or Cisco® Nexus 1000V. The vShield Edge connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, and Load Balancing. Common deployments of vShield Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

This chapter includes the following topics:

- "View the Status of a vShield Edge," on page 68
- "Configure vShield Edge Settings," on page 68
- "Managing Appliances," on page 68
- "Working with Interfaces," on page 70
- "Working with Certificates," on page 73
- "Managing the vShield Edge Firewall," on page 76
- "Managing NAT Rules," on page 81
- "Working with Static Routes," on page 83
- "Managing DHCP Service," on page 84
- "Managing VPN Services," on page 86
- "Managing Load Balancer Service," on page 140
- "About High Availability," on page 145
- "Configure DNS Servers," on page 146
- "Configure Remote Syslog Servers," on page 147
- "Change CLI Credentials," on page 147
- "Upgrade vShield Edge to Large or X-Large," on page 147
- "Download Tech Support Logs for vShield Edge," on page 148
- "Synchronize vShield Edge with vShield Manager," on page 148
- "Redeploy vShield Edge," on page 149

View the Status of a vShield Edge

The status page displays graphs for the traffic flowing through the interfaces of the selected vShield Edge and connection statistics for the firewall and load balancer services.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge instance to check the status for.

6 Click the **Status** tab.

Configure vShield Edge Settings

The Settings page displays detailed information about the selected vShield Edge.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Click the **Configure** tab.

6 Click the **Settings** link.

vShield Edge details, services configured for the vShield Edge, and the HA and DNS configurations are displayed.

What to do next

Change the desired configuration by clicking **Change**.

Managing Appliances

You can add, edit, or delete appliances. A vShield Edge instance remains offline till at least one appliance has been added to it.

Add an Appliance

You must add at least one appliance to vShield Edge before deploying it.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Click the **Configure** tab.

6 Click the **Settings** link.

7 In **Edge Appliances**, click the **Add** ( ) icon.

8 In the Add Edge Appliance dialog box, select the cluster or resource pool and datastore for the appliance.

9 (Optional) Select the host on which the appliance is to be added.

10 (Optional) Select the vCenter folder within which the appliance is to be added.

11 Click **Add**.

Change an Appliance

You can change a vShield Edge appliance.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Click the **Configure** tab.

6 Click the **Settings** link.

7 In **Edge Appliances**, select the appliance to change.

8 Click the **Edit** ( ) icon.

9 In the Edit Edge Appliance dialog box, make the appropriate changes.

10 Click **Save**.

Delete an Appliance

You can delete a vShield Edge appliance.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Click the **Configure** tab.

6 Click the **Settings** link.

7 In **Edge Appliances**, select the appliance to delete.

8 Click the **Delete** ( ) icon.

Working with Interfaces

You install a vShield Edge on a datacenter and can add up to ten internal or uplink interfaces. A vShield Edge must have at least one internal interface before it can be deployed.

Add an Interface

You can add up to ten internal and uplink interfaces to a vShield Edge instance. You must add at least one internal interface for HA to work.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Interfaces** link.

8 Click the **Add** ( ) icon.

9 In the Add Edge Interface dialog box, type a name for the interface.

10 Select **Internal** or **Uplink** to indicate whether this is an internal or external interface.

11 Select the port group or VXLAN virtual wire to which this interface should be connected.

   a Click **Select** next to the **Connected To** field.

   b Depending on what you want to connect to the interface, click the **Virtual Wire**, **Standard Portgroup**, or **Distributed Portgroup** tab.

   c Select the appropriate virtual wire or portgroup.

   d Click **Select**.

12 Select the connectivity status for the interface.

13 In **Configure Subnets**, click the **Add** ( ) icon to add a subnet for the interface.

   An interface can have multiple non-overlapping subnets.

14 In **Add Subnet**, click the **Add** ( ) icon to an IP address.

   If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. vShield Edge considers the Primary IP address as the source address for locally generated traffic.

   You must add an IP address to an interface before using it on any feature configuration.

15 Type the subnet mask for the interface and click **Save**.

16 Change the default MTU if required.

17 In **Options**, select the required options.

Option	Description
Enable Proxy ARP	Supports overlapping network forwarding between different interfaces.
Send ICMP Redirect	Conveys routing information to hosts.

18 Type the fence parameters and click **Add**.

19 Repeat Step 8 through Step 18 to add additional interfaces.

Change Interface Settings

You can change the port group or virtual wire to which an interface is connected, and update the IP address of the interface.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge.

5 Click the **Configure** tab.

6 Click **Interfaces.**

7 Click the **Edit** ( ) icon.

8 Make the required changes.

9 Click **Save**.

Delete an Interface

You can delete a vShield Edge interface.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Interfaces** link

8 Select the interface to delete.

9 Click the **Delete** ( ) icon

Enable an Interface

An interface must be enabled for vShield Edge to isolate the virtual machines within that interface (port group or VXLAN virtual wire).

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Configure** tab.

7 Click the **Interfaces** link

8 Select the interface to enable.

9 Click the **Enable** ( ) icon.

Disable an Interface

You can disable an interface

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Configure** tab.

7 Click **Interfaces** link

8 Select the interface to disable.

9 Click the **Disable** icon.

Working with Certificates

vShield Edge supports self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA.

Configure a CA Signed Certificate

You can generate a CSR and get it signed by a CA. If you generate a CSR at the global level, it is available to all vShield Edges in your inventory.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

Option	Description
To generate a global certificate	a Click **Settings & Reports** from the vShield Manager inventory panel. b Click the **SSL Certificate** tab.
To generate a certificate for a vShield Edge	a Select a datacenter resource from the inventory panel. b Click the **Network Virtualization** tab. c Click the **Edges** link. d Double-click a vShield Edge. e Click the **Configure** tab. f Click the **Certificates** link. g Click **Actions** and select **Generate CSR**.

2 Type your organization unit and name.

3 Type the locality, street, state, and country of your organization.

4 Select the encryption algorithm for communication between the hosts.

Note that SSL VPN-Plus only supports RSA certificates.

5 Edit the default key size if required.

6 For a global certificate, type a description for the certificate.

7 Click **Generate** (at global level) or **OK** (at vShield Edge level).

The CSR is generated and displayed in the Certificates list.

8 Have an online Certification Authority sign this CSR.

9 Import the signed certificate.

Option	Description
To import a signed certificate at the global level	a In the SSL Certificates tab of the vShield Manager user interface, click next to **Import Signed Certificate**. b Click **Browse** and select the CSR file. c Select the certificate type. d Click **Apply**.
To generate a certificate for a vShield Edge	a Copy the contents of the signed certificate. b In the **Certificates** tab, click **Actions** and select **Import Certificate**. c In the Import CSR dialog box, paste the contents of the signed certificate. d Click **OK**.

The CA signed certificate appears in the certificates list.

Add a CA Certificate

By adding a CA certificate, you can become an interim CA for your company. You then have the authority for signing your own certificates.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Configure** tab.

7 Click the **Certificates** link.

8 Click the **Add** ( ) icon and select **CA Certificate.**

9 Copy and paste the certificate contents in the Certificate contents text box.

10 Type a description for the CA certificate.

11 Click **OK**.

You can now sign your own certificates.

Configure a Self-Signed Certificate

You can create, install, and manage self-signed server certificates.

Prerequisites

Verify that you have a CA certificate so that you can sign your own certificates.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Certificates** link.

8 Follow the steps below to generate a CSR.

a Click the **Generate CSR** ( ) icon.

b In Common name, type the IP address or fully qualified domain name (FQDN) of the vShield Manager.

c Type your organization name and unit.

d Type the locality, street, state, and country of your organization.

e Select the encryption algorithm for communication between the hosts.

Note that SSL VPN-Plus only supports RSA certificates. VMware recommends RSA for backward compatibility.

f Edit the default key size if required.

g Type a description for the certificate.

h Click **OK**.

The CSR is generated and displayed in the Certificates list.

9 Verify that the certificate you generated is selected.

10 Click the **Self Sign Certificate** ( ) icon.

11 Type the number of days the self sign certificate is valid for.

12 Click **OK**.

Using Client Certificates

You can create a client certificate through a CAI command or REST call. You can then distribute this certificate to your remote users, who can install the certificate on their web browser

The main benefit of implementing client certificates is that a reference client certificate for each remote user can be stored and checked against the client certificate presented by the remote user. To prevent future connections from a certain user, you can delete the reference certificate from the security server's list of client certificates. Deleting the certificate denies connections from that user.

Add a Certificate Revocation List

A Certificate Revocation List (CRL) is a list of subscribers and their status, which is provided and signed by Microsoft.

The list contains the following items:

- The revoked certificates and the reasons for revocation
- The dates that the certificates are issued
- The entities that issued the certificates
- A proposed date for the next release

When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Certificates** link.

8 Click the **Add** ( ) icon and select **Certificate.**

9 Copy and paste the list.

10 (Optional) Type a description.

11 Click **OK**.

Managing the vShield Edge Firewall

vShield Edge provides firewall protection for incoming and outgoing sessions. The default firewall policy blocks all incoming traffic and allows all outgoing traffic.

In addition to the default firewall policy, you can configure a set of rules to allow or block traffic sessions to and from specific sources and destinations. You can manage the default firewall policy and firewall rule set separately for each vShield Edge instance.

Add a vShield Edge Firewall Rule

You can add a vShield Edge firewall rule for traffic flowing from or to a vShield Edge interface or IP address group.

You can add multiple vShield Edge interfaces and/or IP address groups as the source and destination for firewall rules.

Figure 9-1. Firewall rule for traffic to flow from a vShield Edge interface to an HTTP server

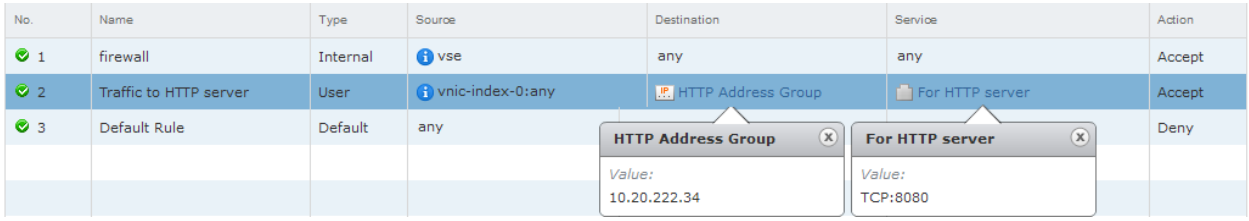
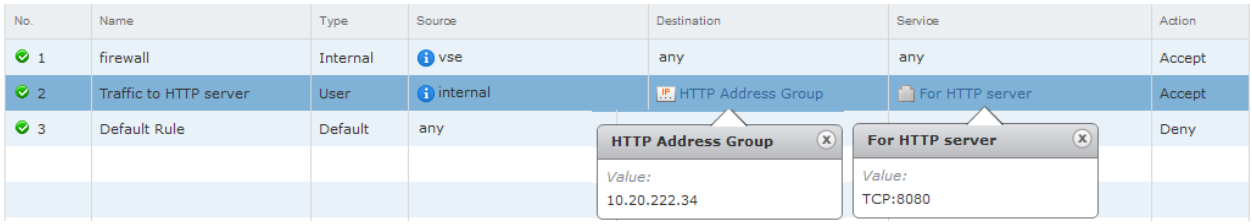
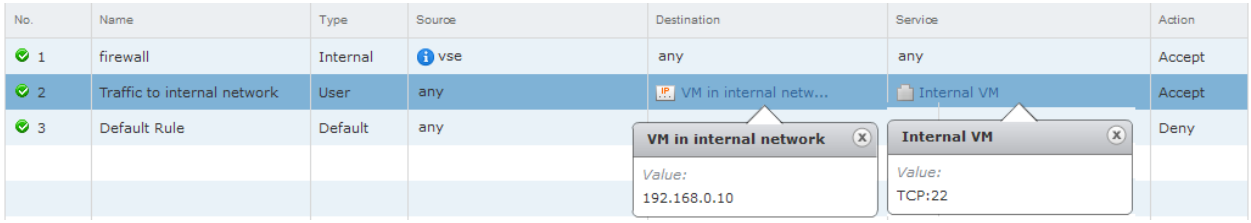


Figure 9-2. Firewall rule for traffic to flow from all internal interfaces (subnets on portgroups connected to internal interfaces) of a vShield Edge to an HTTP Server



NOTE If you select **internal** as the source, the rule is automatically updated when you configure additional internal interfaces.

Figure 9-3. Firewall rule for traffic to allow SSH into a m/c in internal network



Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

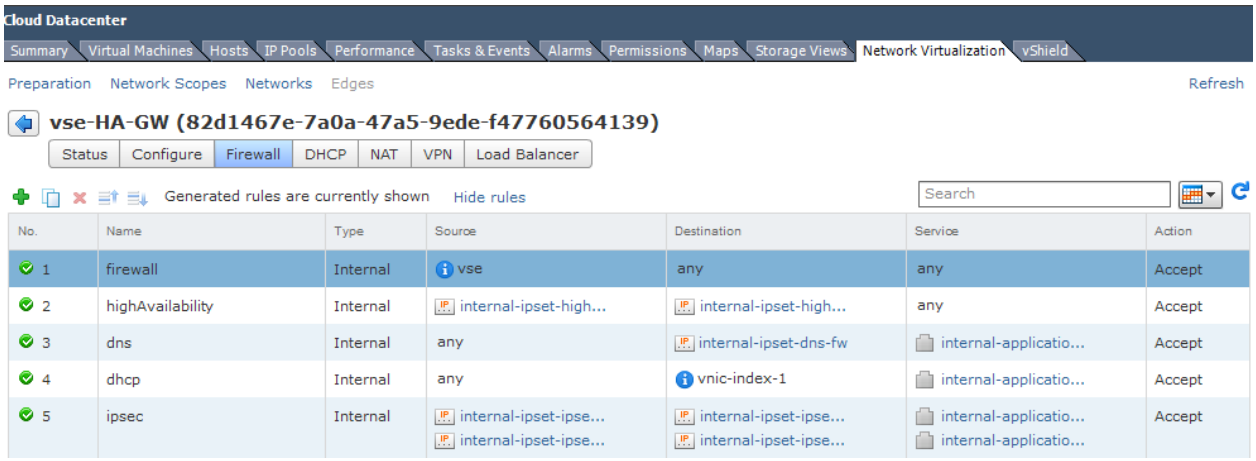
2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Firewall** tab.



7 Do one of the following.

Option	Description
To add a rule at a specific place in the firewall table	a Select a rule. b In the No. column, click and select **Add Above** or **Add Below**. A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.
To add a rule by copying a rule	a Select a rule. b Click the Copy ( ) icon. c Select a rule. d In the No. column, click and select **Paste Above** or **Paste Below**.
To add a rule anywhere in the firewall table	a Click the **Add** ( ) icon. A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.

The new rule is enabled by default.

8 Point to the **Name** cell of the new rule and click .

9 Type a name for the new rule.

10 Point to the **Source** cell of the new rule and click .

a Select **VnicGroup** or **IPAddresses**.

VnicGroup displays vShield Edge (**vse**), **internal** (represents all internal interfaces), **external** (represents all uplink interfaces), and all internal and external interfaces for the vShield Edge. **IPAddresses** displays all IP address groups.

b Select one or more interface or IP address group.

If you select **vse**, the rule applies to traffic generated by the vShield Edge. If you select **internal** or **external**, the rule applies to traffic coming from any internal or uplink interface of the selected vShield Edge instance. The rule is automatically updated when you configure additional interfaces.

If you select **IPAddresses**, you can create a new IP address group. Once you create the new group, it is automatically added to the source column. For information on creating an IPAddress, see "Create an IP Address Group," on page 30.

You can specify the source port by clicking next to **Advance options**. VMware recommends that you avoid specifying the source port from release 5.1 onwards. Instead, you can create a service for a protocol-port combination. See "Create a Service," on page 27.

c Click **OK**.

11 Point to the **Destination** cell of the new rule and click .

a Select **VnicGroup** or **IPAddresses**.

VnicGroup displays vShield Edge (**vse**), **internal** (represents all internal interfaces), **external** (represents all uplink interfaces), and all internal and uplink interfaces for the vShield Edge. **IPAddresses** displays all IP address groups.

b Select one or more interface or IP address group.

If you select **vse**, the rule applies to traffic generated by the vShield Edge. If you select **internal** or **external**, the rule applies to traffic going to any internal or uplink interface of the selected vShield Edge instance. If you add an interface to the vShield Edge instance, the rule automatically applies to the new interface.

If you select **IPAddresses**, you can create a new IP address group. Once you create the new group, it is automatically added to the destination column. For information on creating an IPAddress, see "Create an IP Address Group," on page 30.

c Click **OK**.

12 Point to the **Service** cell of the new rule and click .

Select a service. To create a new service, click **New**. Once you create the new service, it is automatically added to the Service column. For more information on creating a new service, see "Create a Service," on page 27.

NOTE vShield Edge only supports services defined with L3 protocols.

13 Point to the **Action** cell of the new rule and click .

a Click **Deny** to block traffic from or to the specified source and destination.

b Click **Log** to log all sessions matching this rule.

Enabling logging can affect performance.

c Type comments if required.

d Click next to **Advance options**.

e To apply the rule to the translated IP address and services for a NAT rule, select **Translated IP** for **Match on**.

f Click **Enable Rule Direction** and select **Incoming** or **Outgoing**. VMware does not recommend specifying the direction for firewall rules.

g Click **OK**.

14 Click **Publish Changes** to push the new rule to the vShield Edge instance.

What to do next

- Disable a rule by clicking next to the rule number in the **No.** column.
- Display additional columns in the rule table by clicking and selecting the appropriate columns.

Column Name	Information Displayed
Rule Tag	Unique system generated ID for each rule
Log	Traffic for this rule is being logged or not
Stats	Clicking shows the traffic affected by this rule (number of sessions, traffic packets, and size)
Comments	Comments for the rule

- Search for rules by typing text in the Search field.

Change Default Firewall Rule

Default firewall settings apply to traffic that does not match any of the user-defined firewall rules. The default firewall policy blocks all incoming traffic. You can change the default action and logging settings.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to change the default firewall policy.

6 Click the **Firewall** tab.

7 Select the **Default Rule**, which is the last rule in the firewall table.

8 Point to the **Action** cell of the new rule and click .

a Click **Accept** to allow traffic from or to the specified source and destination.

b Click **Log** to log all sessions matching this rule.

Enabling logging can affect performance.

c Type comments if required.

d Click **OK**.

9 Click **Publish Changes**.

Change a vShield Edge Firewall Rule

You can change user-defined firewall rules.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to change a rule.

6 Click the **Firewall** tab.

7 Select the rule to change.

NOTE You cannot change an auto-generated rule or the default rule.

8 Make the desired changes and click **OK**.

9 Click **Publish Changes**.

Change the Priority of a vShield Edge Firewall Rule

You can change the order of user-defined firewall rules to customize traffic flowing through the vShield Edge. For example, suppose you have a rule to allow load balancer traffic. You can now add a rule to deny load balancer traffic from a specific IP address group, and position this rule above the LB allow traffic rule.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to edit a rule.

6 Click the **Firewall** tab.

7 Select the rule for which you want to change the priority.

NOTE You cannot change the priority of auto-generated rules or the default rule.

8 Click the **Move Up** ( ) or **Move Down** ( ) icon.

9 Click **OK**.

10 Click **Publish Changes**.

Delete a vShield Edge Firewall Rule

You can delete a user-defined firewall rule.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to delete a rule.

6 Click the **Firewall** tab.

7 Select the rule to delete.

NOTE You cannot delete an auto-generated rule or the default rule.

8 Click the **Delete** ( ) icon.

Managing NAT Rules

vShield Edge provides network address translation (NAT) service to assign a public address to a computer or group of computers in a private network. Using this technology limits the number of public IP addresses that an organization or company must use, for economy and security purposes. You must configure NAT rules to provide access to services running on privately addressed virtual machines.

The NAT service configuration is separated into source NAT (SNAT) and destination NAT (DNAT) rules.

Add a SNAT Rule

You create a source NAT (SNAT) rule to translate a private internal IP address into a public IP address for outbound traffic.

Prerequisites

The translated (public) IP address must have been added to the vShield Edge interface on which you want to add the rule.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to add a rule.

6 Click the **NAT** tab.

7 Click the **Add** ( ) icon and select **Add SNAT Rule**.

8 Select the interface on which to add the rule.

9 Type the original source IP address in one of the following formats.

Format	Example
IP address	192.168.10.1
IP address range	192.168.10.1-192.168.10.10
IP address/subnet	192.168.10.1/24
any	

10 Type the translated (public) source IP address in one of the following formats.

Format	Example
IP address	192.168.10.1
IP address range	192.168.10.1-192.168.10.10
IP address/subnet	192.168.10.1/24
any	

11 Select **Enabled** to enable the rule.

12 Click **Enable logging** to log the address translation.

13 Click **Add** to save the rule.

14 Click **Publish Changes**.

Add a DNAT Rule

You create a destination (DNAT) rule to map a public IP address to a private internal IP address.

Prerequisites

The original (public) IP address must have been added to the vShield Edge interface on which you want to add the rule.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to add a rule.

6 Click the **NAT** tab.

7 Click the **Add** ( ) icon and select **Add DNAT Rule**.

8 Select the interface on which to apply the DNAT rule.

9 Type the original (public) IP address in one of the following formats.

Format	Example
IP address	192.168.10.1
IP address range	192.168.10.1-192.168.10.10
IP address/subnet	192.168.10.1/24
any	

10 Type the protocol.

11 Type the original port or port range.

Format	Example
Port number	80
Port range	80-85
any	

12 Type the translated IP address in one of the following formats.

Format	Example
IP address	192.168.10.1
IP address range	192.168.10.1-192.168.10.10
IP address/subnet	192.168.10.1/24
any	

13 Type the translated port or port range.

Format	Example
Port number	80
Port range	80-85
any	

14 Select **Enabled** to enable the rule.

15 Select **Enable logging** to log the address translation.

16 Click **Add** to save the rule.

Working with Static Routes

You can set a default gateway and add a static route for your data packets to follow.

Set the Default Gateway

Before you add a static route, you must assign a vShield Edge uplink interface as the default gateway.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Static Routing** tab.

8 In **Default Gateway**, click **Edit**.

9 Select an interface from which the next hop towards the destination network can be reached.

10 Edit the gateway IP if required.

11 Click **Save**.

Add a Static Route

You can add a static route for your data packets to follow.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge.

6 Click the **Configure** tab.

7 Click the **Static Routing** tab

8 Click the **Add** ( ) icon.

9 Select the interface on which you want to add a static route.

10 Type the **Network** in CIDR notation.

11 Type the IP address of the **Next Hop**.

12 For **MTU**, edit the maximum transmission value for the data packets if required.

The MTU cannot be higher than the MTU set on the vShield Edge interface.

13 Click **Add**.

14 Click **Publish Changes**.

Managing DHCP Service

vShield Edge supports IP address pooling and one-to-one static IP address allocation. Static IP address binding is based on the vCenter managed object ID and interface ID of the requesting client.

vShield Edge DHCP service adheres to the following guidelines:

- Listens on the vShield Edge internal interface for DHCP discovery.
- Uses the IP address of the internal interface on vShield Edge as the default gateway address for all clients, and the broadcast and subnet mask values of the internal interface for the container network.

You must restart the DHCP service on client virtual machines in the following situations:

- You changed or deleted a DHCP pool, default gateway, or DNS server.
- You changed the internal IP address of the vShield Edge instance.

Add a DHCP IP Pool

DHCP service requires a pool of IP addresses. An IP pool is a sequential range of IP addresses within the network. Virtual machines protected by vShield Edge that do not have an address binding are allocated an IP address from this pool. An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge instance for which you to add a DHCP pool.

6 Click the **DHCP** tab.

7 In the DHCP Pools panel, click the **Add** ( ) icon.

8 Configure the pool.

Option	Action
Auto Configure DNS	Select to use the DNS service configuration for the DHCP binding.
Lease never expires	Select to bind the address to the MAC address of the virtual machine forever. If you select this, **Lease Time** is disabled.
Start IP	Type the starting IP address for the pool.
End IP	Type the ending IP address for the pool.
Domain Name	Type the domain name of the DNS server. This is optional.
Primary Name Server	If you did not select **Auto Configure DNS**, type the **Primary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
Secondary Name Server	If you did not select **Auto Configure DNS**, type the **Secondary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
Default Gateway	Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the vShield Edge instance is taken as the default gateway. This is optional.
Lease Time	Select whether to lease the address to the client for the default time (1 day), or type a value in seconds. You cannot specify the lease time if you selected **Lease never expires**. This is optional.

9 Click **Add**.

What to do next

Verify that the DHCP service is enabled. The **DHCP Service Status** above the DHCP Pools panel must be set to Enabled.

Add a DHCP Static Binding

If you have services running on a virtual machine and do not want the IP address to be changed, you can bind an IP address to the MAC address of a virtual machine. The IP address you bind must not overlap an IP pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to edit a rule.

6 Click the **DHCP** tab.

7 In the DHCP Bindings panel, click the **Add** ( ) icon.

8 Configure the binding.

Option	Action
Auto Configure DNS	Select to use the DNS service configuration for the DHCP binding.
Lease never expires	Select to bind the address to the MAC address of the virtual machine forever.
Interface	Select the vShield Edge interface to bind.
VM Name	Select the virtual machine to bind.

Option	Action
VM vNIC Index	Select the virtual machine NIC to bind to the IP address.
Host Name	Type the host name of the DHCP client virtual machine.
IP Address	Type the address to which to bind the MAC address of the selected virtual machine.
Domain Name	Type the domain name of the DNS server.
Primary Name Server	If you did not select **Auto Configure DNS**, type the **Primary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
Secondary Name Server	If you did not select **Auto Configure DNS**, type the **Secondary Nameserver** for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the vShield Edge instance is taken as the default gateway.
Lease Time	If you did not select **Lease never expires**, select whether to lease the address to the client for the default time (1 day), or type a value in seconds.

9 Click **Add**.

10 Click **Publish Changes**.

What to do next

Verify that the DHCP service is enabled. The **DHCP Service Status** above the DHCP Pools panel must be set to Enabled.

Managing VPN Services

vShield Edge modules support site-to-site IPSec VPN between a vShield Edge instance and remote sites. vShield Edge modules also support SSL VPN-Plus to allow remote users to access private corporate applications.

1 IPSec VPN Overview on page 86

vShield Edge modules support site-to-site IPSec VPN between a vShield Edge instance and remote sites.

2 SSL VPN-Plus Overview on page 109

With SSL VPN-Plus, remote users can connect securely to private networks behind a NSX Edge gateway. Remote users can access servers and applications in the private networks.

IPSec VPN Overview

vShield Edge modules support site-to-site IPSec VPN between a vShield Edge instance and remote sites.

vShield Edge supports certificate authentication, preshared key mode, IP unicast traffic, and no dynamic routing protocol between the vShield Edge instance and remote VPN routers. Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind a vShield Edge through IPSec tunnels. These subnets and the internal network behind a vShield Edge must have address ranges that do not overlap.

You can deploy a vShield Edge agent behind a NAT device. In this deployment, the NAT device translates the VPN address of a vShield Edge instance to a publicly accessible address facing the Internet. Remote VPN routers use this public address to access the vShield Edge instance.

You can place remote VPN routers behind a NAT device as well. You must provide the VPN native address and the VPN Gateway ID to set up the tunnel. On both ends, static one-to-one NAT is required for the VPN address.

You can have a maximum of 64 tunnels across a maximum of 10 sites.

Configuring IPSec VPN Service

You can set up a vShield Edge tunnel between a local subnet and a peer subnet.

1 Configure IPSec VPN Parameters on page 87

You must configure at least one external IP address on the vShield Edge to provide IPSec VPN service.

2 Enable IPSec VPN Service on page 88

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Configure IPSec VPN Parameters

You must configure at least one external IP address on the vShield Edge to provide IPSec VPN service.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Double-click a vShield Edge instance.

5 Click the **VPN** tab.

6 Ensure that you are in the IPSec VPN tab.

7 Click the **Add** ( ) icon.

The Add IPSec VPN dialog box opens.

8 Type a name for the IPSec VPN.

9 Type the IP address of the vShield Edge instance in **Local Id**. This will be the peer Id on the remote site.

10 Type the IP address of the local endpoint.

If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.

11 Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.

12 Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID

13 Type the IP address of the peer site in Peer Endpoint. If you leave this blank, vShield Edge waits for the peer device to request a connection.

14 Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.

15 Select the Encryption Algorithm.

16 In Authentication Method, select one of the following:

Option	Description
PSK (Pre Shared Key)	Indicates that the secret key shared between vShield Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.
Certificate	Indicates that the certificate defined at the global level is to be used for authentication.

17 Type the shared key in if anonymous sites are to connect to the VPN service.

18 Click **Display Shared Key** to display the key on the peer site.

19 In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the vShield Edge to establish a shared secret over an insecure communications channel.

20 Edit the default MTU if required.

21 Select whether to enable or disable the Perfect Forward Secrecy (PFS) threshold. In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key.

22 Click **OK**.

vShield Edge creates a tunnel from the local subnet to the peer subnet.

What to do next

Enable the IPSec VPN service.

Enable IPSec VPN Service

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Ensure that you are in the IPSec VPN tab.

8 In IPSec VPN Service Status, click **Enable**.

What to do next

Click **Enable Logging** to log the traffic flow between the local subnet and peer subnet.

Edit IPSec VPN Service

You can edit an IPSec VPN service.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Ensure that you are in the IPSec VPN tab.

8 Select the IPSec service that you want to edit.

9 Click the **Edit** ( ) icon.

The Edit IPSec VPN dialog box opens.

10 Make the appropriate edits.

11 Click **OK**.

Delete IPSec Service

You can delete an IPSec service.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Ensure that you are in the IPSec VPN tab.

8 Select the IPSec service that you want to delete

9 Click the **Delete** ( ) icon.

The selected IPSec service is deleted.

Enable IPSec Service

You must enable an IPSec service for traffic to flow between the local and peer subnets.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Ensure that you are in the IPSec VPN tab.

8 Select the IPSec service that you want to enable.

9 Click the **Enable** ( ) icon.

The selected service is enabled.

Disable IPSec Service

You can disable an IPSec service.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Ensure that you are in the IPSec VPN tab.

8 Select the IPSec service that you want to disable.

9 Click the **Disable** ( ) icon.

The selected service is disabled.

vShield Edge VPN Configuration Examples

This scenario contains configuration examples for a basic point-to-point IPSEC VPN connection between a vShield Edge and a Cisco or WatchGuard VPN on the other end.

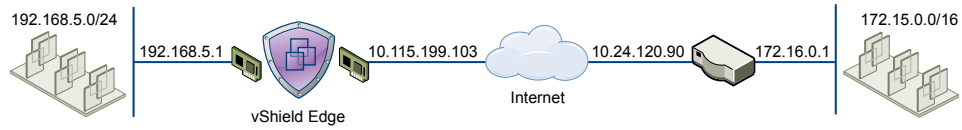
For this scenario, vShield Edge connects the internal network 192.168.5.0/24 to the internet. The vShield Edge interfaces are configured as follows:

- Uplink interface: 10.115.199.103
- Internal interface: 192.168.5.1

The remote gateway connects the 172.16.0.0/16 internal network to the internet. The remote gateway interfaces are configured as follows:

- Uplink interface: 10.24.120.90/24
- Internal interface: 172.16.0.1/16

Figure 9-4. vShield Edge connecting to a remote VPN gateway



NOTE For vShield Edge to vShield Edge IPSEC tunnels, you can use the same scenario by setting up the second vShield Edge as the remote gateway.

Terminology

IPSec is a framework of open standards. There are many technical terms in the logs of the NSX Edge and other VPN appliances that you can use to troubleshoot the IPSEC VPN.

These are some of the standards you may encounter:

- ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.
- Oakley is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.
- IKE (Internet Key Exchange) is a combination of ISAKMP framework and Oakley. NSX Edge provides IKEv1.
- Diffie-Hellman (DH) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. VSE supports DH group 2 (1024 bits) and group 5 (1536 bits).

IKE Phase 1 and Phase 2

IKE is a standard method used to arrange secure, authenticated communications.

Phase 1 Parameters

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys. The Phase 1 parameters used by NSX Edge are:

- Main mode
- TripleDES / AES [Configurable]
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret [Configurable]
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying
- ISAKMP aggressive mode disabled

Phase 2 Parameters

IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSec tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange). The IKE Phase 2 parameters supported by NSX Edge are:

- TripleDES / AES [Will match the Phase 1 setting]
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

Transaction ModeSamples

NSX Edge supports Main Mode for Phase 1 and Quick Mode for Phase 2.

NSX Edge proposes a policy that requires PSK, 3DES/AES128, sha1, and DH Group 2/5. The peer must accept this policy; otherwise, the negotiation phase fails.

Phase 1: Main Mode Transactions

This example shows an exchange of Phase 1 negotiation initiated from a NSX Edge to a Cisco device.

The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Main Mode.

1 NSX Edge to Cisco

- proposal: encrypt 3des-cbc, sha, psk, group5(group2)
- DPD enabled

2 Cisco to NSX Edge

- contains proposal chosen by Cisco
- If the Cisco device does not accept any of the parameters the NSX Edge sent in step one, the Cisco device sends the message with flag NO_PROPOSAL_CHOSEN and terminates the negotiation.

3 NSX Edge to Cisco

- DH key and nonce

4 Cisco to NSX Edge

- DH key and nonce

5 NSX Edge to Cisco (Encrypted)

- include ID (PSK)

6 Cisco to NSX Edge (Encrypted)

- include ID (PSK)
- If the Cisco device finds that the PSK doesn't match, the Cisco device sends a message with flag INVALID_ID_INFORMATION; Phase 1 fails.

Phase 2: Quick Mode Transactions

The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Quick Mode.

1 NSX Edge to Cisco

NSX Edge proposes Phase 2 policy to the peer. For example:

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
```

2 Cisco to NSX Edge

Cisco device sends back NO_PROPOSAL_CHOSEN if it does not find any matching policy for the proposal. Otherwise, the Cisco device sends the set of parameters chosen.

3 NSX Edge to Cisco

To facilitate debugging, you can enable IPSec logging on the NSX Edge and enable crypto debug on Cisco (debug crypto isakmp <level>).

Configuring IPSec VPN Service Example

You must configure VPN parameters and then enable the IPSEC service.

Procedure

1 Configure vShield Edge VPN Parameters Example on page 93

You must configure at least one external IP address on the vShield Edge to provide IPSec VPN service.

2 Enable IPSec VPN Service Example on page 94

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Configure vShield Edge VPN Parameters Example

You must configure at least one external IP address on the vShield Edge to provide IPSec VPN service.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Double-click a vShield Edge instance.

5 Click the **VPN** tab.

6 Ensure that you are in the IPSec VPN tab.

7 Click the **Add** ( ) icon.

The Add IPSec VPN dialog box opens.

8 Type a name for the IPSec VPN.

9 Type the IP address of the vShield Edge instance in **Local Id**. This will be the peer Id on the remote site.

10 Type the IP address of the local endpoint.

If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.

11 Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.

12 Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID

13 Type the IP address of the peer site in Peer Endpoint. If you leave this blank, vShield Edge waits for the peer device to request a connection.

14 Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.

15 Select the Encryption Algorithm.

16 In Authentication Method, select one of the following:

Option	Description
PSK (Pre Shared Key)	Indicates that the secret key shared between vShield Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.
Certificate	Indicates that the certificate defined at the global level is to be used for authentication.

17 Type the shared key in if anonymous sites are to connect to the VPN service.

18 Click **Display Shared Key** to display the key on the peer site.

19 In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the vShield Edge to establish a shared secret over an insecure communications channel.

20 Change the MTU threshold if required.

21 Select whether to enable or disable the Perfect Forward Secrecy (PFS) threshold. In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key.

22 Click **OK**.

vShield Edge creates a tunnel from the local subnet to the peer subnet.

What to do next

Enable the IPSec VPN service.

Enable IPSec VPN Service Example

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Ensure that you are in the IPSec VPN tab.

7 In IPSec VPN Service Status, click **Enable**.

What to do next

Click **Enable Logging** to log the traffic flow between the local subnet and peer subnet.

Using a Cisco 2821 Integrated Services Router

The following describes configurations performed using Cisco IOS.

Procedure

1 Configure Interfaces and Default Route

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
```

```
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

2 Configure IKE Policy

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
     pre-share
Router(config-isakmp)# exit
```

3 Match Each Peer with Its Pre-Shared Secret

```
Router# config term
Router(config)# crypto isakmp key vshield
    address 10.115.199.103
Router(config-isakmp)# exit
```

4 Define the IPSEC Transform

```
Router# config term
Router(config)# crypto ipsec transform-set
     myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

5 Create the IPSEC Access List

```
Router# config term
Enter configuration commands, one per line.
     End with CNTL/Z.
Router(config)# access-list 101 permit ip
     172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

6 Bind the Policy with a Crypto Map and Label It

In the following example, the crypto map is labeled MYVPN

```
Router# config term
Router(config)# crypto map MYVPN 1
      ipsec-isakmp
% NOTE: This new crypto map will remain
      disabled until a peer and a valid
      access list have been configured.
Router(config-crypto-map)# set transform-set
      myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
      10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

Example: Example Configuration

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
      esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
```

```
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
       0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end
```

Using a Cisco ASA 5510

Use the following output to configure a Cisco ASA 5510.

```
ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
```

```
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
      192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
      172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
      udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
      mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
      sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
```

```
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end
```

Configuring a WatchGuard Firebox X500

You can configure your WatchGuard Firebox X500 as a remote gateway.

NOTE Refer to your WatchGuard Firebox documentation for exact steps.

Procedure

1 In Firebox System Manager, select **Tools > Policy Manager** > .

2 In Policy Manager, select **Network > Configuration**.

3 Configure the interfaces and click **OK**.

4 (Optional) Select **Network > Routes** to configure a default route.

5 Select **Network > Branch Office VPN > Manual IPSec** to configure the remote gateway.

6 In the IPSec Configuration dialog box, click **Gateways** to configure the IPSEC Remote Gateway.

7 In the IPSec Configuration dialog box, click **Tunnels** to configure a tunnel.

8 In the IPSec Configuration dialog box, click **Add** to add a routing policy.

9 Click **Close**.

10 Confirm that the tunnel is up.

Troubleshooting vShield Edge Configuration Example

Use this information to help you troubleshoot negotiation problems with your setup.

Successful Negotiation (both Phase 1 and Phase 2)

The following examples display a successful negotiating result between vShield Edge and a Cisco device.

vShield Edge

From the vShield Edge command line interface (ipsec auto -status, part of show service ipsec command):

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

    Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

    IKE Peer: 10.20.129.80
    Type : L2L        Role    : responder
    Rekey : no        State   : MM_ACTIVE
    Encrypt : 3des    Hash    : SHA
    Auth : preshared  Lifetime: 28800
    Lifetime Remaining: 28379
```

Phase 1 Policy Not Matching

The following lists Phase 1 Policy Not Matching Error logs.

NSX Edge

NSX Edge hangs in STATE_MAIN_I1 state. Look in /var/log/messages for information showing that the peer sent back an IKE message with "NO_PROPOSAL_CHOSEN" set.

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
      import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    SPI size: 0
```

```
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      "s1-c1" #1: ignoring informational payload,
       type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

If debug crypto is enabled, an error message is printed to show that no proposals were accepted.

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
      IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=0) with payloads : HDR + SA (1)
      + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
      payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
      FSM error history (struct &0xd8355a60)  <state>, <event>:
      MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
      MM:9e0e4511 terminating:  flags 0x01000002, refcnt 0,
      tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
      delete/delete with reason message
```

Phase 2 Not Matching

The following lists Phase 2 Policy Not Matching Error logs.

NSX Edge

NSX Edge hangs at STATE_QUICK_I1. A log message shows that the peer sent a NO_PROPOSAL_CHOSEN message.

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
      0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
      ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    next payload
```

```
      type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
      ignoring informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
```

Cisco

Debug message show that Phase 1 is completed, but Phase 2 failed because of policy negotiation failure.

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
      IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
      for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
      + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
      total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

PFS Mismatch

The following lists PFS Mismatch Error logs.

NSX Edge

PFS is negotiated as part of Phase 2. If PFS does not match, the behavior is similar to the failure case described in "Phase 2 Not Matching," on page 101.

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
      (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
```

```
      informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
      91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | processing informational NO_PROPOSAL_CHOSEN (14)
```

Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, sending delete/delete with
      reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
      + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

PSK not Matching

The following lists PSK Not Matching Error logs

NSX Edge

PSK is negotiated in the last round of Phase 1. If PSK negotiation fails, NSX Edge state is STATE_MAIN_I4. The peer sends a message containing INVALID_ID_INFORMATION.

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
      "s1-c1" #1: transition from state STATE_MAIN_I3 to
      state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      STATE_MAIN_I4: ISAKMP SA established
      {auth=OAKLEY_PRESHARED_KEY
      cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
      Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
      initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
      {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
      pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      ignoring informational payload, type INVALID_ID_INFORMATION
      msgid=00000000
```

Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
      IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
      + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
      + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
      + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, Received encrypted Oakley Main Mode
      packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, ERROR, had problems decrypting
      packet, probably due to mismatched pre-shared key.
      Aborting
```

Packet Capture for a Successful Negotiation

The following lists a packet capture session for a successful negotiation between NSX Edge and a Cisco device.

```
No.     Time        Source        Destination   Protocol Info
9203    768.394800  10.20.129.80  10.20.131.62  ISAKMP  Identity Protection
                                                        (Main Mode)
Frame 9203 (190 bytes on wire, 190 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 148
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 0
      Next payload: NONE (0)
      Payload length: 72
      Proposal number: 0
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 2
      Transform payload # 0
         Next payload: Transform (3)
         Payload length: 32
         Transform number: 0
```

```
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): 1536 bit MODP group (5)
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): Alternate 1024-bit MODP group (2)
  Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

No.     Time        Source        Destination   Protocol Info
9204    768.395550  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 104
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 52
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 1
      Next payload: NONE (0)
      Payload length: 40
      Proposal number: 1
```

```
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 1
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Group-Description (4): Alternate 1024-bit MODP group (2)
         Authentication-Method (3): PSK (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
  Vendor ID: Microsoft L2TP/IPSec VPN Client
    Next payload: NONE (0)
    Payload length: 24
    Vendor ID: Microsoft L2TP/IPSec VPN Client

No.     Time        Source        Destination   Protocol Info
9205    768.399599  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                      (Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data


No.     Time        Source        Destination   Protocol Info
9206    768.401192  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                      (Main Mode)
Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
```

```
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: Vendor ID (13)
    Payload length: 24
    Nonce Data
  Vendor ID: CISCO-UNITY-1.0
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: CISCO-UNITY-1.0
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
    Next payload: Vendor ID (13)
    Payload length: 12
    Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Vendor ID: CISCO-CONCENTRATOR
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: CISCO-CONCENTRATOR

No.     Time        Source        Destination   Protocol Info
9207    768.404990  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
```

```
  Encrypted payload (40 bytes)

No.     Time        Source        Destination   Protocol Info
9208    768.405921  10.20.131.62  10.20.129.80  ISAKMP   Identity Protection
                                                          (Main Mode)
Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 84
  Encrypted payload (56 bytes)

No.     Time        Source        Destination   Protocol Info
9209    768.409799  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9210    768.411797  10.20.131.62  10.20.129.80  ISAKMP   Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
```

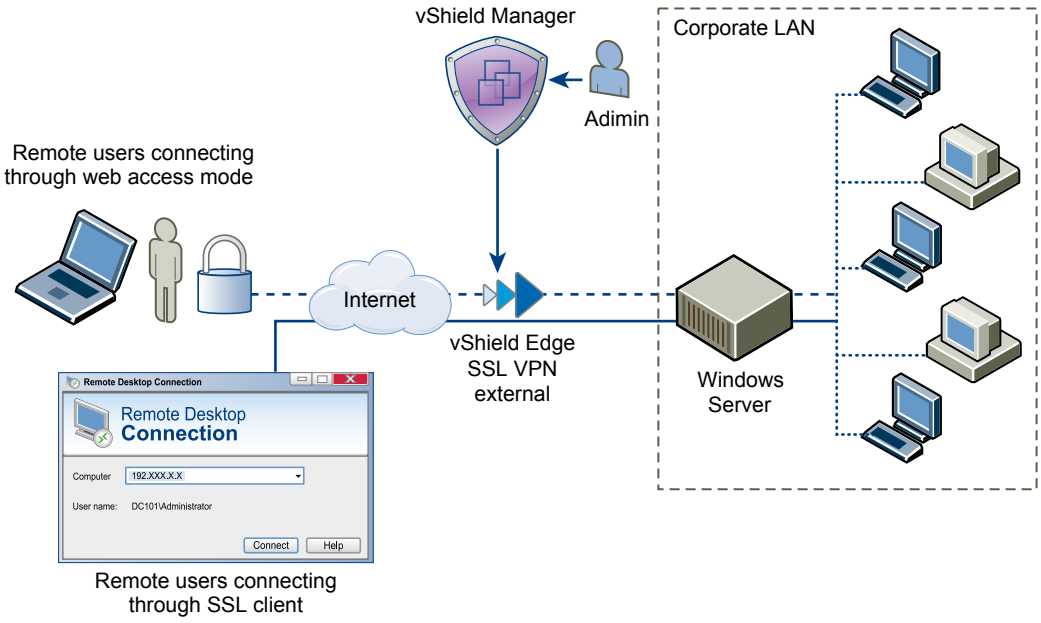
```
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9211    768.437057  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 52
  Encrypted payload (24 bytes)
```

SSL VPN-Plus Overview

With SSL VPN-Plus, remote users can connect securely to private networks behind a NSX Edge gateway. Remote users can access servers and applications in the private networks.



Configure Network Access SSL VPN-Plus

In network access mode, a remote user can access private networks after downloading and installing an SSL client.

Prerequisites

The SSL VPN gateway requires port 443 to be accessible from external networks and the SSL VPN client requires the vShield Edge gateway IP and port 443 to be reachable from client system.

Procedure

1 Add SSL VPN-Plus Server Settings on page 110

You must select the external vShield Edge interface on which you want to enable SSL VPN.

2 Add an IP Pool on page 111

The remote user is assigned a virtual IP address from the IP pool that you add.

3 Add private network on page 111

Add the network that you want the remote user to be able to access after logging in to SSL VPN.

4 Add Authentication on page 112

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

5 Add Installation Package on page 115

Create an installation package of the SSL VPN-Plus client for the remote user. The user can use this installation package to get SSL VPN-Plus on his/her desktop. Windows, MAC, and Linux desktops are supported.

6 Add a User on page 116

Add users that can login to SSL VPN-Plus.

7 Enable the SSL VPN-Plus Service on page 116

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

8 Install SSL Client on Remote Site on page 117

This section describes the procedure a remote user can follow on his/her desktop after SSL VPN-Plus is configured. Windows, MAC, and Linux desktops are supported.

Add SSL VPN-Plus Server Settings

You must select the external vShield Edge interface on which you want to enable SSL VPN.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Edges** tab.

7 Click the **VPN** tab.

8 Click the **SSL VPN-Plus** tab.

9 In the **Configure** panel, click **Server Settings**.

10 Click **Change.**

The Change Server Settings dialog box opens.

11 Select the vShield Edge external interface on which you want to enable SSL VPN-Plus. Select **ANY - 0.0.0.0** to enable SSL VPN-Plus on all interfaces of the selected vShield Edge.

12 Edit the port number if required. This port number is required to configure the installation package.

13 Select the encryption method.

14 (Optional) From the Server Certificates table, select the server certificate that you want to add.

15 Click **OK.**

Add an IP Pool

The remote user is assigned a virtual IP address from the IP pool that you add.

Procedure

1 Click **IP Pool** and then click the **Add** ( ) icon.

2 Type the begin and end IP address for the IP pool.

3 Type the netmask of the IP pool.

4 Type the IP address which is to add the routing interface in the vShield Edge gateway.

5 (Optional) Type a description for the IP pool.

6 Select whether to enable or disable the IP pool.

7 (Optional) In the **Advanced** panel, type the DNS name.

8 (Optional) Type the secondary DNS name.

9 Type the connection-specific DNS suffix for domain based host name resolution.

10 Type the WINS server address.

11 Click **OK**.

Add private network

Add the network that you want the remote user to be able to access after logging in to SSL VPN.

Procedure

1 Click **Private Networks** and then click the **Add** ( ) icon.

2 Type the private network IP address.

3 Type the netmask of the private network.

4 (Optional) Type a description for the network.

5 Specify whether you want to send private network and internet traffic over the SSL VPN-Plus enabled vShield Edge or directly to the private server by bypassing the vShield Edge.

6 If you selected **Send traffic over the tunnel**, select **Enable TCP Optimization** to optimize the internet speed.

Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the internet. This results in application layer data being encapsulated twice in two separate TCP streams. When packet loss occurs (which happens even under optimal internet conditions), a performance degradation effect called TCP-over-TCP meltdown occurs. In essence, two TCP instruments are correcting a single packet of IP data, undermining network throughput and causing connection timeouts. TCP Optimization eliminates this TCP-over-TCP problem, ensuring optimal performance.

7 Type the port numbers that you want to open for the remote user to access the corporate internal servers/machines like 3389 for RDP, 20/21 for FTP, and 80 for http. If you want to give unrestricted access to the user, you can leave the **Ports** field blank.

8 Specify whether you want to enable or disable the private network.

9 Click **OK**.

What to do next

- Add a corresponding firewall rule to allow the private network traffic.

Add Authentication

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

The maximum time to authenticate over SSL VPN is 3 minutes. This is because non-authentication timeout is 3 minutes and is not a configurable property. So in scenarios where AD authentication timeout is set to more than 3 minutes or there are multiple authentication servers in chain authorization and the time taken for user authentication is more than 3 minutes, you will not be authenticated.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Authentication** from the left panel.

2 Click the **Add** ( ) icon.

3 Select the type of authentication server.

4 Depending on the type of authentication server you selected, complete the following fields.

- AD authentication server

Table 9-1. AD Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the authentication server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.

Table 9-1. AD Authentication Server Options (Continued)

Option	Description
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **sAMAccountName**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.
Use this server for secondary authentication	If selected, this AD server is used as the second level of authentication.
Terminate Session if authenticati on fails	When selected, the session is ended if authentication fails.

- LDAP authentication server

Table 9-2. LDAP Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **sAMAccountName**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

- RADIUS authentication server

Table 9-3. RADIUS authentication server options

Option	Description
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Secret	Shared secret specified while adding the authentication agent in the RSA security console.
Retype secret	Retype the shared secret.
NAS IP Address	IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.
Retry Count	Number of times the RADIUS server is to be contacted if it does not respond before the authentication fails.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- RSA-ACE authentication server

Table 9-4. RSA-ACE authentication server options

Option	Description
Timeout	Period in seconds within which the AD server must respond.
Configuration File	Click **Browse** to select the `sdconf.rec` file that you downloaded from the RSA Authentication Manager.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Source IP Address	IP address of the NSX Edge interface through which the RSA server is accessible.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- Local authentication server

Table 9-5. Local authentication server options

Option	Description
Enable password policy	If selected, defines a password policy. Specify the required values.
Enable password policy	If selected, defines an account lockout policy. Specify the required values. 1 In Retry Count, type the number of times a remote user can try to access his or her account after entering an incorrect password.

Table 9-5. Local authentication server options (Continued)

Option	Description
	2 In Retry Duration, type the time period in which the remote user's account gets locked on unsuccessful login attempts. For example, if you specify Retry Count as 5 and Retry Duration as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute. 3 In Lockout Duration, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

Add Installation Package

Create an installation package of the SSL VPN-Plus client for the remote user. The user can use this installation package to get SSL VPN-Plus on his/her desktop. Windows, MAC, and Linux desktops are supported.

Procedure

1 In the SSL VPN-Plus tab, click **Installation Package** and then click the **Add** ( ) icon.

2 Type a profile name for the installation package.

3 In **Gateway**, type the IP address or FQDN of the public interface of vShield Edge.

This IP address or FQDN is binded to the SSL client. When the client is installed, this IP address or FQDN is displayed on the SSL client.

4 Type the port number that you specified in the server settings for SSL VPN-Plus. See "Add SSL VPN-Plus Server Settings," on page 110.

5 (Optional) To bind additional vShield Edge uplink interfaces to the SSL client,

a Click the **Add** ( ) icon.

b Type the IP address and port number.

c Click **OK**.

6 The installation package is created for Windows operating system by default. Select Linux or Mac to create an installation package for Linux or Mac operating systems as well.

7 (Optional) Enter a description for the installation package.

8 Select **Enable** to display the installation package on the Installation Package page.

9 Select the following options as appropriate.

Option	Description
Start client on logon	The SSL VPN client is started when the remote user logs on to his system.
Allow remember password	Enables the option
Enable silent mode installation	Hides installation commands from remote user.

Option	Description
Hide SSL client network adapter	Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN installation package.
Hide client system tray icon	Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
Create desktop icon	Creates an icon to invoke the SSL client on the user's desktop.
Enable silent mode operation	Hides the pop-up that indicates that installation is complete.
Server security certificate validation	The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.

10 Click **OK.**

Add a User

Add users that can login to SSL VPN-Plus.

Procedure

1 In the SSL VPN-Plus tab, click **Users** and then click the **Add** ( ) icon.

2 Type the user ID and password.

3 Retype the password.

4 (Optional) Type the first name of the user.

5 (Optional) Type the last name of the user.

6 (Optional) Type a description for the user.

7 In Password Details, select **Password never expires** to always keep the same password for the user.

8 Click **OK**.

Enable the SSL VPN-Plus Service

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

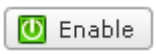
3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click the 

icon.

The SSL VPN-Plus dashboard displays the status of the service, number of active SSL VPN sessions, and session statistics and data flow details.

Install SSL Client on Remote Site

This section describes the procedure a remote user can follow on his/her desktop after SSL VPN-Plus is configured. Windows, MAC, and Linux desktops are supported.

Procedure

1 On the client site, the remote user can type (`https://`*ExternalEdgeInterfaceIP*`/sslvpn-plus/`) in a browser window where *ExternalEdgeInterfaceIP* is the IP address of the Edge external interface where you enabled SSL VPN-Plus.

2 Login to the portal using the user name and password created in the Users section.

3 Click Full Access tab.

The SSL client is downloaded.

4 Login to the SSL client with the credentials specified in the Users section.

The remote user can now access the private network.

Configure Web Access SSL VPN-Plus

In web access mode, a remote user can access private networks without downloading an SSL client.

Procedure

1 Add SSL VPN-Plus Server Settings on page 117

You must select the external vShield Edge interface on which you want to enable SSL VPN.

2 Create a Web Resource on page 118

You can add a web access server that the remote user can connect to via a web browser.

3 Add a User on page 118

Add users that can login to SSL VPN-Plus.

4 Add Authentication on page 119

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

5 Enable the SSL VPN-Plus Service on page 125

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Add SSL VPN-Plus Server Settings

You must select the external vShield Edge interface on which you want to enable SSL VPN.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Edges** tab.

7 Click the **VPN** tab.

8 Click the **SSL VPN-Plus** tab.

9 In the **Configure** panel, click **Server Settings**.

10 Click **Change.**

The Change Server Settings dialog box opens.

11 Select the vShield Edge external interface on which you want to enable SSL VPN-Plus. Select **ANY - 0.0.0.0** to enable SSL VPN-Plus on all interfaces of the selected vShield Edge.

12 Edit the port number if required. This port number is required to configure the installation package.

13 Select the encryption method.

14 (Optional) From the Server Certificates table, select the server certificate that you want to add.

15 Click **OK.**

Create a Web Resource

You can add a web access server that the remote user can connect to via a web browser.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Web Resource**.

9 Click the **Add** ( ) icon.

The Add Web Resource dialog box opens.

10 Type a name for the web resource.

11 Type the URL of the web resource that you want the remote user to access.

12 Depending on whether the remote user wants to read from or write to the web resource, select the **HTTPMethod**.

13 Type the description for the web resource. This description is displayed on the web portal when the remote user accesses the web resource.

14 Select **Enable** to enable the web resource. The web resource must be enabled for the remote user to access it.

What to do next

Add a local user or authentication for an external user.

Add a User

Add users that can login to SSL VPN-Plus.

Procedure

1 In the SSL VPN-Plus tab, click **Users** and then click the **Add** ( ) icon.

2 Type the user ID and password.

3 Retype the password.

4 (Optional) Type the first name of the user.

5 (Optional) Type the last name of the user.

6 (Optional) Type a description for the user.

7 In Password Details, select **Password never expires** to always keep the same password for the user.

8 Click **OK**.

Add Authentication

Instead of a local user, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

The maximum time to authenticate over SSL VPN is 3 minutes. This is because non-authentication timeout is 3 minutes and is not a configurable property. So in scenarios where AD authentication timeout is set to more than 3 minutes or there are multiple authentication servers in chain authorization and the time taken for user authentication is more than 3 minutes, you will not be authenticated.

- Add AD Authentication Server on page 122

  You can add an AD authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

- Add LDAP Authentication Server on page 123

  You can add an AD authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

- Add RADIUS Authentication Server on page 124

  You can add an RADIUS authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

- Add RSA-ACE Authentication Server on page 124

  You can add an RSA-ACE authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

- Add Local Authentication Server on page 125

  You can add a local authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the **SSL Vpn-Plus** tab, select **Authentication** from the left panel.

2 Click the **Add** ( ) icon.

3 Select the type of authentication server.

4 Depending on the type of authentication server you selected, complete the following fields.

- AD authentication server

Table 9-6. AD Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the authentication server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.

Table 9-6. AD Authentication Server Options (Continued)

Option	Description
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **`sAMAccountName`**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.
Use this server for secondary authentication	If selected, this AD server is used as the second level of authentication.
`Terminate Session if authenticati on fails`	When selected, the session is ended if authentication fails.

- LDAP authentication server

Table 9-7. LDAP Authentication Server Options

Option	Description
Enable SSL	Enabling SSL establishes an encrypted link between a web server and a browser.
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Search base	Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
Bind DN	User on the external server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.
Bind Password	Password to authenticate the AD user.
Retype Bind Password	Retype the password.
Login Attribute Name	Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **`sAMAccountName`**.
Search Filter	Filter values by which the search is to be limited. The search filter format is *attribute operator value*.

Table 9-7. LDAP Authentication Server Options (Continued)

Option	Description
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authentication fails`	When selected, the session is ended if authentication fails.

- RADIUS authentication server

Table 9-8. RADIUS authentication server options

Option	Description
IP Address	IP address of the external server.
Port	Displays default port name. Edit if required.
Timeout	Period in seconds within which the AD server must respond.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Secret	Shared secret specified while adding the authentication agent in the RSA security console.
Retype secret	Retype the shared secret.
NAS IP Address	IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.
Retry Count	Number of times the RADIUS server is to be contacted if it does not respond before the authentication fails.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- RSA-ACE authentication server

Table 9-9. RSA-ACE authentication server options

Option	Description
Timeout	Period in seconds within which the AD server must respond.
Configuration File	Click **Browse** to select the `sdconf.rec` file that you downloaded from the RSA Authentication Manager.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Source IP Address	IP address of the NSX Edge interface through which the RSA server is accessible.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
`Terminate Session if authenticatio n fails`	When selected, the session is ended if authentication fails.

- Local authentication server

Table 9-10. Local authentication server options

Option	Description
Enable password policy	If selected, defines a password policy. Specify the required values.
Enable password policy	If selected, defines an account lockout policy. Specify the required values. 1 In Retry Count, type the number of times a remote user can try to access his or her account after entering an incorrect password. 2 In Retry Duration, type the time period in which the remote user's account gets locked on unsuccessful login attempts. For example, if you specify Retry Count as 5 and Retry Duration as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute. 3 In Lockout Duration, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.
Status	Select **Enabled** or **Disabled** to indicate whether the server is enabled.
Use this server for secondary authentication	If selected, this server is used as the second level of authentication.
Terminate Session if authentication fails	When selected, the session is ended if authentication fails.

Add AD Authentication Server

You can add an AD authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the SSL VPN-Plus tab, click **Authentication** and then click the **Add** ( ) icon.

2 In **Type**, select **AD**.

3 Type the IP address of the external server.

4 Type the port number for the AD server.

5 Select **Enable SSL** to enable the SSL service on the specified server.

6 In **Timeout Period**, type the period in seconds within which the AD server must respond.

7 Select **Enabled** or **Disabled** to indicate whether the server is enabled.

8 Type the search base to indicate the part of the external directory tree to search.

The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

9 Type the bind DN.

Bind DN is the user on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.

10 Type the bind password to authenticate the AD user.

11 Retype the bind password.

12 In **Login attribute name**, type the name against which the user ID entered by the remote user is matched with.

For Active Directory, the login attribute name is **sAMAccountName**.

13 In **Search Filter**, type the filter values by which you want to limit the search.

The search filter format is *attribute operator value*.

14 Select **Use this server for secondary authentication** if you want to use this AD server as the second level of authentication.

15 Click **OK**.

Add LDAP Authentication Server

You can add an AD authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the SSL VPN-Plus tab, click **Authentication** and then click the **Add** ( ) icon.

2 In **Type**, select **LDAP**.

3 Type the IP address of the external server.

4 Type the port number for the LDAP server.

5 Select **Enable SSL** to enable the SSL service on the specified server.

6 Type the timeout period in seconds.

7 Select **Enabled** or **Disabled** to indicate whether the server is enabled.

8 Type the search base to indicate the part of the external directory tree to search.

The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

9 Type the bind DN.

Bind DN is the user on the external AD server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating LDAP users. When the DN is returned, the DN and password are used to authenticate the LDAP user.

10 Type and retype the bind password to authenticate the LDAP user.

11 In **Login attribute name**, type the name against which the user ID entered by the remote user is matched with.

For Active Directory, the login attribute name is **sAMAccountName**.

12 In **Search Filter**, type the filter values by which you want to limit the search.

The search filter format is *attribute operator value*.

13 Select **Use this server for secondary authentication** if you want to use this LDAP server as the second level of authentication.

14 Click **OK**.

Add RADIUS Authentication Server

You can add an RADIUS authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the SSL VPN-Plus tab, click **Authentication** and then click the **Add** ( ) icon.

2 In **Type**, select **RADIUS**.

3 Type the IP address of the RSA Radius server.

4 Type the port number for the RADIUS server.

5 Type the timeout period in seconds.

6 Select **Enabled** or **Disabled** to indicate whether the server is enabled.

7 Type and re-type the shared secret specified while adding the authentication agent in the RSA security console.

8 Type the NAS IP address for authentication.

9 Type the number of times the RADIUS server is to be contacted if it does not respond.

10 Select **Use this server for secondary authentication** if you want to use this server as the second level of authentication.

Select **Terminate Session if authentication fails** if required.

11 Click **OK**.

Add RSA-ACE Authentication Server

You can add an RSA-ACE authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the SSL VPN-Plus tab, click **Authentication** and then click the **Add** ( ) icon.

2 In **Type**, select **RSA-ACE**.

3 (Optional) Type the timeout period in seconds for the RSA server.

4 In **Configuration File**, browser to and select the `sdconf.rec` file that you downloaded from the RSA Authentication Manager.

5 Select **Enabled** or **Disabled** to indicate whether the server is enabled.

6 In the **Advanced** section, type the IP address of the vShield Edge interface through which the RSA server is accessible.

7 Select **Use this server for secondary authentication** if you want to use this server as the second level of authentication.

Select **Terminate Session if authentication fails** if required.

8 Click **OK**.

Add Local Authentication Server

You can add a local authentication server to bound to the SSL gateway. All users in the bounded authenticated server will be authenticated.

Procedure

1 In the SSL VPN-Plus tab, click **Authentication** and then click the **Add** ( ) icon.

2 In **Type**, select **LOCAL**.

3 To define a password policy, select **Password Policy** and specify the required values.

4 To define an account lockout policy, select **Enable** next to **Account Lockout Policy**.

   a In **Retry Count**, type the number of times a remote user can try to access his or her account after entering an incorrect password.

   b In **Retry Duration**, type the time period in which the remote user's account gets locked on unsuccessful login attempts.

   For example, if you specify **Retry Count** as 5 and **Retry Duration** as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute.

   c In **Lockout Duration**, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.

5 Select **Enabled** or **Disabled** to indicate whether the server is enabled.

6 Select **Use this server for secondary authentication** if you want to use this server as the second level of authentication.

   Select **Terminate Session if authentication fails** if required.

7 Click **OK**.

Enable the SSL VPN-Plus Service

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

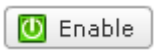
3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click the 

icon.

   The SSL VPN-Plus dashboard displays the status of the service, number of active SSL VPN sessions, and session statistics and data flow details.

Working with IP Pools

You can add, edit, or delete an IP pool.

Add an IP Pool

The remote user is assigned a virtual IP address from the IP pool that you add.

Procedure

1 Click **IP Pool** and then click the **Add** ( ) icon.

2 Type the begin and end IP address for the IP pool.

3 Type the netmask of the IP pool.

4 Type the IP address which is to add the routing interface in the vShield Edge gateway.

5 (Optional) Type a description for the IP pool.

6 Select whether to enable or disable the IP pool.

7 (Optional) In the **Advanced** panel, type the DNS name.

8 (Optional) Type the secondary DNS name.

9 Type the connection-specific DNS suffix for domain based host name resolution.

10 Type the WINS server address.

11 Click **OK**.

Edit an IP Pool

You can edit an IP pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **IP Pool**.

9 Select the IP pool that you want to edit.

10 Select the IP pool that you want to edit.

11 Click the **Edit** ( ) icon.

The Edit IP Pool dialog box opens.

12 Make the required edits.

13 Click **OK**.

Delete an IP Pool

You can delete an IP pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **IP Pool**.

8 Select the IP pool that you want to delete.

9 Click the **Delete** ( ) icon.

The selected IP pool is deleted.

Enable an IP Pool

You can enable an IP pool if you want an IP address from that pool to be assigned to the remote user.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **IP Pool**.

8 Select the IP pool that you want to enable

9 Click the **Enable** ( ) icon.

The selected IP pool is enabled.

Disable an IP Pool

You can disable an IP pool if you do not want the remote user to be assigned an IP address from that pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **IP Pool**.

8 Select the IP pool that you want to disable

9 Click the **Disable** ( ) icon.

The selected IP pool is disabled.

Change the Order of an IP Pool

SSL VPN assigns an IP address to a remote user based on the order of the IP pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **IP Pool**.

8 Select the IP pool that you want to change the order for.

9 Click the **Move Up** ( ) or Move Down ( ) icon.

Working with Private Networks

You can add, edit, or delete a private network that a remote user can access.

Add private network

Add the network that you want the remote user to be able to access after logging in to SSL VPN.

Procedure

1 Click **Private Networks** and then click the **Add** ( ) icon.

2 Type the private network IP address.

3 Type the netmask of the private network.

4 (Optional) Type a description for the network.

5 Specify whether you want to send private network and internet traffic over the SSL VPN-Plus enabled vShield Edge or directly to the private server by bypassing the vShield Edge.

6 If you selected **Send traffic over the tunnel**, select **Enable TCP Optimization** to optimize the internet speed.

Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the internet. This results in application layer data being encapsulated twice in two separate TCP streams. When packet loss occurs (which happens even under optimal internet conditions), a performance degradation effect called TCP-over-TCP meltdown occurs. In essence, two TCP instruments are correcting a single packet of IP data, undermining network throughput and causing connection timeouts. TCP Optimization eliminates this TCP-over-TCP problem, ensuring optimal performance.

7 Type the port numbers that you want to open for the remote user to access the corporate internal servers/machines like 3389 for RDP, 20/21 for FTP, and 80 for http. If you want to give unrestricted access to the user, you can leave the **Ports** field blank.

8 Specify whether you want to enable or disable the private network.

9 Click **OK**.

What to do next

- Add a corresponding firewall rule to allow the private network traffic.

Delete a Private Network

You can delete a private network

Procedure

1. In the vSphere Client, select **Inventory > Hosts & Clusters**.
2. Select a datacenter resource from the inventory panel.
3. Click the **Network Virtualization** tab.
4. Click the **Edges** tab.
5. Double-click a vShield Edge gateway.
6. Click the **VPN** tab.
7. Click the **SSL VPN-Plus** tab.
8. In the **Configure** panel, click **Private Networks**.
9. Click the network that you want to delete.
10. Click the **Delete** ( ) icon

    The selected network is deleted.

Enable a Private Network

When you enable a private network, the remote user can access it through SSL VPN-Plus.

Procedure

1. In the vSphere Client, select **Inventory > Hosts & Clusters**.
2. Select a datacenter resource from the inventory panel.
3. Click the **Network Virtualization** tab.
4. Click the **Edges** tab.
5. Double-click a vShield Edge gateway.
6. Click the **VPN** tab.
7. Click the **SSL VPN-Plus** tab.
8. In the **Configure** panel, click **Private Networks**.
9. Click the network that you want to enable.
10. Click the **Enable** icon ( ).

    The selected network is enabled.

Disable a Private Network

When you disable a private network, the remote user cannot access it through SSL VPN-Plus.

Procedure

1. In the vSphere Client, select **Inventory > Hosts & Clusters**.
2. Select a datacenter resource from the inventory panel.

3 Click the **Edge** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **Private Networks**.

8 Click the network that you want to disable.

9 Click the **Disable** ( ) icon.

The selected network is disabled.

Change the Sequence of a Private Network

SSL VPN-Plus allows remote users to access private networks in the sequence in which they are displayed on the Private Networks panel.

If you select **Enable TCP Optimization** for a private network, some applications such as FTP in Active mode may not work within that subnet. To add an FTP server configured in Active mode, you must add another private network for that FTP server with TCP Optimization disabled. Also, the active TCP private network must be enabled, and must be placed above the subnet private network

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Double-click a vShield Edge gateway.

5 Click the **VPN** tab.

6 Click the **SSL VPN-Plus** tab.

7 In the **Configure** panel, click **Private Networks**.

8 Click the **Change Order** ( ) icon

The Change Order dialog box opens.

9 Select the network that you want to change the order of.

10 Click the **Move Up** ( )or **Move Down** ( ) icon.

11 Click **OK**.

Working with Installation Packages

You can add, delete, or edit an installation package for the SSL client.

Add Installation Package

Create an installation package of the SSL VPN-Plus client for the remote user. The user can use this installation package to get SSL VPN-Plus on his/her desktop. Windows, MAC, and Linux desktops are supported.

Procedure

1 In the SSL VPN-Plus tab, click **Installation Package** and then click the **Add** ( ) icon.

2 Type a profile name for the installation package.

3 In **Gateway**, type the IP address or FQDN of the public interface of vShield Edge.

This IP address or FQDN is binded to the SSL client. When the client is installed, this IP address or FQDN is displayed on the SSL client.

4 Type the port number that you specified in the server settings for SSL VPN-Plus. See "Add SSL VPN-Plus Server Settings," on page 110.

5 (Optional) To bind additional vShield Edge uplink interfaces to the SSL client,

a Click the **Add** ( ) icon.

b Type the IP address and port number.

c Click **OK**.

6 The installation package is created for Windows operating system by default. Select Linux or Mac to create an installation package for Linux or Mac operating systems as well.

7 (Optional) Enter a description for the installation package.

8 Select **Enable** to display the installation package on the Installation Package page.

9 Select the following options as appropriate.

Option	Description
Start client on logon	The SSL VPN client is started when the remote user logs on to his system.
Allow remember password	Enables the option
Enable silent mode installation	Hides installation commands from remote user.
Hide SSL client network adapter	Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN installation package.
Hide client system tray icon	Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
Create desktop icon	Creates an icon to invoke the SSL client on the user's desktop.
Enable silent mode operation	Hides the pop-up that indicates that installation is complete.
Server security certificate validation	The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.

10 Click **OK.**

Edit an Installation Package

You can edit an installation package.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **Installation Package**.

9 Select the installation package that you want to edit.

10 Click the Edit ( ) icon.

The Edit Installation Package dialog box opens.

11 Make the required edits.

12 Click **OK**.

Delete an Installation Package

You can delete an installation package.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **Installation Package**.

9 Select the installation package that you want to delete.

10 Click the **Delete** ( ) icon.

The selected IP pool is deleted.

Working with Users

You can add, edit, or delete users from the local database.

Add a User

Add users that can login to SSL VPN-Plus.

Procedure

1 In the SSL VPN-Plus tab, click **Users** and then click the **Add** ( ) icon.

2 Type the user ID and password.

3 Retype the password.

4 (Optional) Type the first name of the user.

5 (Optional) Type the last name of the user.

6 (Optional) Type a description for the user.

7 In Password Details, select **Password never expires** to always keep the same password for the user.

8 Click **OK**.

Edit a User

You can edit the details for a user except for the user ID.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **Users**.

9 Click the **Edit** ( ) icon.

The Edit User dialog box opens.

10 Make the required edits.

11 Click **OK**.

Delete a User

You can delete a user.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **Users**.

9 Select the user that you want to delete.

10 Click the **Delete** ( ) icon.

The selected user is deleted.

Change the Password for a User

You can change the password for a user.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 In the **Configure** panel, click **Users**.

9 Click the **Change Password** icon.

The change Password dialog box opens.

10 Type the new password.

11 Type the new password again.

12 Click Change password on next login to change the password when the user logs in to his system next time.

13 Click **OK**.

Edit Client Configuration

You can change the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Client Configuration**.

The Change Client Configuration dialog box opens.

9 Select the **Tunneling Mode**.

In split tunnel mode, only the VPN flows through the vShield Edge gateway. In full tunnel, the vShield Edge gateway becomes the remote user's default gateway and all traffic (VPN, local, and internet) flows through this gateway.

10 If you selected the full tunnel mode:

a Select **Exclude local subnets** to exclude local traffic from flowing through the VPN tunnel.

b Type the IP address for the default gateway of the remote user's system.

11 Select **Enable auto reconnect** if you would like the remote user to automatically reconnect to the SSL VPN client after getting disconnected.

12 Select **Start on login** if you want the SSL Client login screen to be displayed as soon as the remote user logs in to his computer.

13 Select **Client upgrade notification** for the remote user to get a notification when an upgrade for the client is available. The remote user can then choose to install the upgrade.

14 Click **OK**.

Working with Login and Logoff Scripts

You can bind a login or logoff script to the vShield Edge gateway.

Add a Script

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Click the **Add** ( ) icon.

The Add Login-Logoff script dialog box opens.

10 In **Script**, click **Browse** and select the script you want to bind to the vShield Edge gateway.

11 Select the **Type** of script.

Option	Description
Login	Performs the script action when remote user logs in to SSL VPN.
Logoff	Performs the script action when remote user logs out of SSL VPN.
Both	Performs the script action both when remote user logs in and logs out of SSL VPN

12 Type a description for the script.

13 Select **Enabled** to enable the script.

14 Click **OK**.

Edit a Script

You can edit the type, description, and status of a login or logoff script that is bound to the vShield Edge gateway.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Select a script.

10 Click the **Edit** ( ) icon.

The Edit Login-Logoff script dialog box opens.

11 Make the appropriate changes.

12 Click **OK**.

Delete a Script

You can delete a login or logoff script.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Select a script.

10 Click the **Delete** ( ) icon.

Enable a Script

You must enable a script for it to work.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Select a script.

10 Click the **Enable** ( ) icon.

Disable a Script

You can disable a login/logoff script.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Select a script.

10 Click the **Disable** ( ) icon.

Refresh Scripts

After you add or delete a script, you can refresh the Login/Logoff Scripts page.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Select a script.

10 Click the Refresh ( ) icon.

Change the Order of a Script

You can change the order of a script. For example, suppose you have a login script for opening gmail.com in Internet Explorer placed above a login script for opening yahoo.com. When the remote user logs in to SSL VPN, gmail.com is displayed before yahoo.com. If you now reverse the order of the login scripts, yahoo.com is displayed before gmail.com.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Login/Logoff Scripts**.

9 Click the **Change Order** ( ) icon

The Change Order dialog box opens.

10 Select the script that you want to change the order of.

11 Click the **Move Up** ( )or **Move Down** ( ) icon.

12 Click **OK**.

SSL VPN-Plus Logs

SSL VPN-Plus gateway logs are sent to the syslog server configured on the vShield Edge appliance. SSL VPN-Plus client logs are stored in the following directory on the remote user's computer: `%PROGRAMFILES %/VMWARE/SSL VPN Client/`.

Edit General Settings

You can edit the default VPN settings.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **General Settings**.

The Change General Settings dialog box opens.

9 Make required selections.

Select	To
Prevent multiple logon using same username	Allow a remote user to login only once with a username
Enable compression	Enable TCP based intelligent data compression and improve data transfer speed.
Enable logging	Maintain a log of the traffic passing through the SSL VPN gateway.
Force virtual keyboard	Allow remote users to enter web or client login information only via the virtual keyboard.
Randomize keys of virtual keyboard	Make the virtual keyboard keys random.
Enable forced timeout	Disconnect the remote user after the specified timeout period is over. Type the timeout period in minutes.
Session idle timeout	If there is no activity on the user session for the specified period, end the user session after that period is over.
User notification	Type a message to be displayed to the remote user after he logs in.
Enable public URL access	Allow remote user to access any site which is not configured (and not listed on web portal) by administrator.

10 Click **OK**.

Edit Web Portal Design

You can edit the client banner bound to the SSL VPN client.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **VPN** tab.

7 Click the **SSL VPN-Plus** tab.

8 Click **Portal Customization**.

The Change Web Portal Design dialog box opens.

9 Type the portal title.

10 Type the remote user's company name.

11 In **Logo**, click **Change** and select the image file for the remote user's logo.

12 In **Colors**, click the color box next to numbered item for which you want to change the color, and select the desired color.

13 Click **OK**.

Managing Load Balancer Service

vShield Edge provides load balancing for TCP, HTTP, and HTTPS traffic. Load balancing, up to Layer 7, enables Web application auto scaling.

You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 8090 is the default listening port for TCP, port 80 is the default port for HTTP, and port 443 is the default port for HTTPs.

Configure Load Balancer Service

You can create a pool of backend servers and specify the services that the pool would support. You can then associate two or more virtual machines behind a server pool for the load balancer service.

Procedure

1 Add a Server Pool on page 140

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages healthcheck monitors and load balancer distribution methods.

2 Add Virtual Servers on page 143

Add a vShield Edge internal or uplink interface as a virtual server.

Add a Server Pool

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages healthcheck monitors and load balancer distribution methods.

Procedure

1 Open the Add Pool Wizard on page 140

Open the Add Pool wizard to start the process of adding a load balancer pool.

2 Name the Load Balancer Pool on page 141

Provide a descriptive name and an optional description for the load balancer pool.

3 Select and Configure Services for the Pool on page 141

You can select and configure the services to be supported by this pool.

4 Define Health Check Parameters on page 141

A health check checks that all servers in the server pool are alive and answering queries.

5 Add Servers on page 142

Add backend servers to the pool.

6 Review Settings and Add Pool on page 142

Before you add the server pool, review the settings you entered.

Open the Add Pool Wizard

Open the Add Pool wizard to start the process of adding a load balancer pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Ensure that you are in the **Pools** tab.

8 Click the **Add** ( ) icon.

The Add Pool wizard opens.

Name the Load Balancer Pool

Provide a descriptive name and an optional description for the load balancer pool.

Procedure

1 In the Name and Description page of the Add pool wizard, type a name for the load balancer pool.

2 (Optional) Type a description for the pool.

3 Click **Next**.

Select and Configure Services for the Pool

You can select and configure the services to be supported by this pool.

Procedure

1 In the Services page of the Add pool wizard, click **Enable** for each service to support.

2 Select a balancing method for each enabled service.

Option	Description
IP_HASH	Selects a server based on a hash of the source and destination IP address of each packet.
LEAST_CONN	Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.
ROUND_ROBIN	Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed.
URI	The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down.

3 (Optional) Change the default port for each enabled service, if necessary.

4 Repeat Step 1 through Step 3 for each additional service to enable for the pool.

5 Click **Next**.

Define Health Check Parameters

A health check checks that all servers in the server pool are alive and answering queries.

vShield Edge supports three health check modes.

Option	Description
TCP	TCP connection check.
HTTP	The GET / default method is used to detect server status. Only responses 2xx and 3xx are valid. Other responses (including a lack of response) indicates a server failure.
SSL	Tests servers using SSLv3 client hello messages. The server is considered valid only when the response contains server hello messages.

Procedure

1 In the Health Check page of the Add pool wizard, change the monitor port if required for each service that is to be supported by this pool.

The health check monitor port is also used as the service port.

2 Select the health check mode for each service.

3 The table below lists the health check parameters. You can change the default values if required.

Parameter	Description
Interval	Interval at which a server is pinged.
Timeout	Time within which a response from the server must be received.
Health Threshold	Number of consecutive successful health checks before a server is declared operational.
Unhealth Threshold	Number of consecutive unsuccessful health checks before a server is declared dead.

4 For HTTP, type the URI referenced in the HTTP ping requests.

5 Click **Next**.

Add Servers

Add backend servers to the pool.

Procedure

1 In the Members page of the Add Pool wizard, click the **Add** ( ) icon.

2 Type the IP address of the server.

3 Type the weight to indicate the ratio of how many requests are to be served by this backend server.

4 Change the default port and monitor port for the server if required.

5 Click **Add**.

6 Repeat Step 1steps through Step 5 to add additional servers.

7 Click **Next**.

Review Settings and Add Pool

Before you add the server pool, review the settings you entered.

Procedure

1 In the Ready to Complete page of the Add Pool wizard, review the settings for the server pool.

2 Click **Previous** to modify the settings.

3 Click **Finish** to accept the settings and add the pool.

4 Click **Publish Changes** for the pool configuration to take effect.

Add Virtual Servers

Add a vShield Edge internal or uplink interface as a virtual server.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Click the **Virtual Servers** tab.

8 Click the **Add** ( ) icon.

9 Type a name for the virtual server.

10 (Optional) Type a description for the virtual server.

11 Type the IP address of a vShield Edge interface.

12 Select the pool to be associated with the virtual server.

The services supported by the selected pool appear.

13 In **Services**, click **Enable** for each service to be supported.

14 Change the default Port, Persistence Method, Cookie Name, and Cookie Mode values as required.

15 Click **Enabled** to enable the virtual server.

16 Click **Enable logging**.

Edit a Server Pool

You can edit a server pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Ensure that you are in the Pool tab.

8 Select the pool to edit.

9 Click the **Edit** ( ) icon.

10 Make the appropriate changes and click **Finish**.

Delete a Server Pool

You can delete a server pool.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Ensure that you are in the Pool tab.

8 Select the pool to edit.

9 Click the **Delete** ( ) icon.

10 Make the appropriate changes and click **Finish**.

Edit a Virtual Server

You can edit a virtual server.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Click **Virtual Servers** tab.

8 Select the virtual server to edit.

9 Click the **Edit** ( ) icon.

10 Make the appropriate changes and click **Finish**.

Delete a Virtual Server

You can delete a virtual server.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Load Balancer** tab.

7 Click **Virtual Servers** tab.

8 Select the virtual server to delete.

9 Click the **Delete** ( ) icon.

About High Availability

High Availability (HA) ensures that a vShield Edge appliance is always available on your virtualized network. You can enable HA either when installing vShield Edge or on an installed vShield Edge instance.

Stateful High Availability

The primary vShield Edge appliance is in the active state and the secondary appliance is in the standby state. All vShield Edge services run on the active appliance. The primary appliance maintains a heartbeat with the standby appliance and sends service updates through an internal interface.

If a heartbeat is not received from the primary appliance within the specified time (default value is 6 seconds), the primary appliance is declared dead. The standby appliance moves to the active state, takes over the interface configuration of the primary appliance, and starts the vShield Edge services that were running on the primary appliance. When the switch over takes place, a system event is displayed in the **System Events** tab of Settings & Reports. Load Balancer and VPN services need to re-establish TCP connection with vShield Edge, so service is disrupted for a short while. Virtual wire connections and firewall sessions are synched between the primary and standby appliances, so there is no service disruption during switch over.

If the vShield Edge appliance fails and a bad state is reported, HA force syncs the failed appliance in order to revive it. When revived, it takes on the configuration of the now-active appliance and stays in a standby state. If the vShield Edge appliance is dead, you must delete the appliance and add a new one.

vShield Edge replicates the configuration of the primary appliance for the standby appliance or you can manually add two appliances. VMware recommends that you create the primary and secondary appliances on separate resource pools and datastores. If you create the primary and secondary appliances on the same datastore, the datastore must be shared across all hosts in the cluster for the HA appliance pair to be deployed on different ESX hosts. If the datastore is a local storage, both virtual machines are deployed on the same host.

vShield Edge ensures that the two HA vShield Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host). Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the vShield Edge HA so that they can communicate with each other. You can specify management IP addresses to override the local links.

If syslog servers are configured, logs on the active appliance are sent to the syslog servers.

vSphere High Availability

vShield Edge HA is compatible with vSphere HA. If the host on which a vShield Edge instance is running dies, the vShield Edge is restarted on the standby host thereby ensuring the vShield Edge HA pair is still available to take another failover.

If vSphere HA is not leveraged, the active-standby vShield Edge HA pair will survive one fail-over. However, if another fail-over happens before the second HA pair was restored, vShield Edge availability can be compromised.

For more information on vSphere HA, see *vSphere Availability*.

Change HA Configuration

You can change the HA configuration that you had specified while installing vShield Edge.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge for which you want to specify the syslog servers.

6 Click the **Configure** tab.

7 Click the **Settings** link

8 In the **HA Configuration** panel, click **Change**.

9 In the Change HA Configuration dialog box, make changes as appropriate.

10 Click **OK**.

Configure DNS Servers

You can configure external DNS servers to which vShield Edge can relay name resolution requests from clients. vShield Edge will relay client application requests to the DNS servers to fully resolve a network name and cache the response from the servers.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click a vShield Edge instance.

6 Click the **Status** tab.

7 In the **DNS Configuration** panel, click **Change**.

8 Click **Enable DNS Service** to enable the DNS service.

9 Type IP addresses for both DNS servers.

10 Change the default cache size if required.

11 Click **Enable Logging** to log DNS traffic.

Generated logs are sent to the syslog server.

12 Select the log level.

13 Click **Ok**.

Configure Remote Syslog Servers

You can configure one or two remote syslog servers. vShield Edge events and logs related to firewall events that flow from vShield Edge appliances are sent to the syslog servers.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Double-click the vShield Edge instance for which you want to specify the syslog servers.

6 Click the **Status** tab.

7 In the **Details** panel, click **Change** next to Syslog servers.

8 Type the IP address of both remote syslog servers.

9 Click **Add** to save the configuration.

Change CLI Credentials

You can edit the credentials to be used for logging in to the Command Line Interface (CLI).

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Select a vShield Edge instance.

6 Click the **More Actions** ( ) icon and select **Change CLI Credentials**.

7 Make the appropriate edits.

8 Click **OK**.

Upgrade vShield Edge to Large or X-Large

If you installed a compact vShield Edge instance, you can upgrade it to a large or x-large vShield Edge instance.

Prerequisites

- A compact vShield Edge instance requires 256 MB memory and 200 MB disk space.
- A large vShield Edge instance requires 1 GB memory and 256 MB disk space.
- An x-large vShield Edge instance requires 8 GB memory and 256 MB disk space. An x-large vShield Edge instance is recommended for an environment where the Load Balancer service is being used on millions of concurrent sessions.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Select a compact vShield Edge instance.

6 Click the **More Actions** ( ) icon and select **Upgrade to Large** or **Upgrade to X-Large**.

The vShield Edge instance is upgraded.

Download Tech Support Logs for vShield Edge

You can download technical support logs for each vShield Edge instance. If high availability is enabled for the vShield Edge instance, support logs from both vShield Edge virtual machines are downloaded.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** tab.

5 Select a vShield Edge instance.

6 Click the **More Actions** ( ) icon and select **Download Tech Support Logs**.

7 After the tech support logs are generated, click **Download**.

8 In the Select location for download dialog box, browse to the directory where you want to save the log file.

9 Click **Save**.

10 Click **Close**.

Synchronize vShield Edge with vShield Manager

If a vShield service is not responding, or if a service is out of sync with what vShield Manager is showing, you can send a synchronization request from vShield Manager to vShield Edge.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Select a vShield Edge instance.

6 Click the **More Actions** ( ) icon and select **Force Sync**.

Redeploy vShield Edge

If vShield services do not work as expected after a force sync, you can redeploy the vShield Edge instance.

Procedure

1 In the vSphere Client, select **Inventory > Hosts & Clusters**.

2 Select a datacenter resource from the inventory panel.

3 Click the **Network Virtualization** tab.

4 Click the **Edges** link.

5 Select a vShield Edge instance.

6 Click the **More Actions** ( ) icon and select **Redeploy Edge**.

The vShield Edge virtual machine is replaced with a new virtual machine and all services are restored. If redeploy does not work, power off the vShield Edge virtual machine and redeploy vShield Edge again.

NOTE Redeploy may not work in the following cases.

- Resource pool on which the vShield Edge was installed is no longer in the vCenter inventory or its MoId (identifier in vCenter Server) has changed.
- Datastore on which the vShield Edge was installed is corrupted/unmounted or in-accessible.
- dvportGroups on which the vShield interfaces were connected are no longer in the vCenter inventory or their MoId (identifier in vCenter server) has changed.

If any of the above is true, you must update the Moid of the resource pool, datastore, or dvPortGroup using a REST API call. See *vShield API Programming Guide*.

Service Insertion Management 10

VMware partners can integrate NetX services with their VMware virtual environment.

After you design the services that you want to offer, you can implement your service virtual machine and create vendor templates which contain the settings and configuration parameters for the levels of an offered service or different services that you provide.

Your service administrator registers your service manager and service with vShield Manager, and monitors the health and performance of the service.

Service consumers can create a service profile to configure a service to work on a region of the network, and edit vendor specific attributes of the service. They can then bind a service to a virtual wire.

This chapter includes the following topics:

- "Inserting a Network Services," on page 151
- "Change Service Precedence," on page 154
- "Edit a Service Manager," on page 154
- "Delete a Service Manager," on page 155
- "Edit a Service," on page 155
- "Delete a Service," on page 155
- "Edit a Service Profile," on page 155
- "Delete a Service Profile," on page 156

Inserting a Network Services

VMware solution partners (vendors) can integrate their solutions with vShield Manager, and automate the provision and consumption of these solutions. Network services can be inserted at the network edge and work with vShield Edge services such as load balancing and vShield Edge firewall.

Procedure

1 Register Service Manager on page 152

You must register the solution provider's service manager with vShield Manager. Your service manager manages your services in the vShield environment.

2 Register Service on page 152

Register the partner service that you want to register with vShield Manager.

3 Create Service Profiles on page 153

Service consumers can create a service profile to represent a combined setting of the configuration required by the virtualization infrastructure to run the service and the provider specific configuration for the service. Examples of provider specific configuration include network-region-awareness, quality of service, etc. You can also edit provider specific attributes of the service.

4 Deploy Service on page 154

You can deploy a service on a virtual wire.

Register Service Manager

You must register the solution provider's service manager with vShield Manager. Your service manager manages your services in the vShield environment.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Click the **Managers** tab.

4 Click the **Add** ( ) icon.

The Create Service Manager dialog box opens.

5 Type a name for the service manager.

6 (Optional) Type a description for the service manager.

7 (Optional) In **Administrative URL**, type the URL of the solution provider's service manager.

8 (Optional) In **Base API URL**, type the URL of the web site where the service manager's REST APIs are available.

The base API URL needs to be specified only for solutions that have been integrated directly with the VMware virtual environment.

9 (Optional) In **Vendor Details**, type the solution provider's ID and name.

10 In **Credentials**, type the username and password for logging in to the service manager.

11 Click **OK**.

The service manager you created is added to the service manager table.

Register Service

Register the partner service that you want to register with vShield Manager.

Prerequisites

The VMware solution provider must have provided a service template to you. The template may define the level of the service you are adding or provide other information about the service.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Click the **Services** tab.

4 Click the **Add** ( ) icon.

The Service Wizard opens.

5 Type a name for the service.

6 Select a category for the service you are adding.

7 Select the service manager for the service.

8 Type a description for the service.

9 Click **Next**.

10 To add a service configuration or other vendor information, click the **Add** ( ) icon.

The Create Vendor Template dialog box opens.

11 Type the ID and name of the vendor template.

12 Type a description for the template.

13 Click **OK**.

14 In Service Configuration, click Next.

15 Review the service and configuration details.

16 Click **Finish**.

The service is added to the service table.

Create Service Profiles

Service consumers can create a service profile to represent a combined setting of the configuration required by the virtualization infrastructure to run the service and the provider specific configuration for the service. Examples of provider specific configuration include network-region-awareness, quality of service, etc. You can also edit provider specific attributes of the service.

A service can have multiple service profiles.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Ensure that you are in the **Services** tab.

3 Click the service for which you want to create a profile.

4 Click the **Service Profiles** tab.

5 Click the **Add** (I icon.

The Create Service Profile dialog box opens.

6 Type a name and description for the profile.

7 Select the vendor template for which you want to edit the attributes.

8 Edit the required attribute values.

9 Click **OK**.

Deploy Service

You can deploy a service on a virtual wire.

Procedure

1 Select a datacenter resource from the vShield Manager inventory panel.

2 Click the **Network Virtualization** tab.

3 Click the **Virtual Wires** tab.

4 In the **Name** column, click the virtual wire on which you want to deploy a service.

5 In the **Available Services** panel, click **Enable Services**.

6 In the Apply Service Profile to this Network dialog box, select the service and service profile that you want to apply.

7 Click **Apply**.

Change Service Precedence

Services are applied in the order in which they exist in the service table. You can move a service up or down in the table.

Prerequisites

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Click the **Services** tab.

4 Select the service that you want to move.

5 Click .

6 Click the **Move Up** ( ) or **Move Down** ( ) icon to position the service appropriately.

7 Click **OK**.

Edit a Service Manager

You can edit a service manager.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Ensure that you are in the **Managers** tab.

3 Click the service manager that you want to edit.

4 Click **Edit**.

The Edit Service Manager dialog box opens.

5 Make the required edits.

6 Click **OK**.

Delete a Service Manager

You can delete a service manager.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Ensure that you are in the **Managers** tab.

4 Click the service manager that you want to delete.

5 Click the **Delete** icon ( ).

Edit a Service

You can edit a service if required.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Ensure that you are in the **Services** tab.

3 Click the service that you want to edit.

4 Click **Edit**.

The Edit Service dialog box opens.

5 Make the required edits.

6 Click **OK**.

Delete a Service

You can delete a service.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Click the **Services** tab.

4 Click the service that you want to delete.

5 Click the **Delete** icon ( ).

Edit a Service Profile

You can edit the description, template, or attributes of a service profile.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Ensure that you are in the **Services** tab.

4 Click the service for which you want to create a profile.

5 Click the **Service Profiles** tab.

6 Click the profile that you want to edit.

7 Click **Edit**.

The Edit Service Profile dialog box opens.

8 Make the required edits.

9 Click **OK**.

Delete a Service Profile

You can delete a service profile.

Procedure

1 Click **Settings & Reports** from the vShield Manager inventory panel.

2 Click **Service Insertion**.

3 Ensure that you are in the **Services** tab.

4 Click the service for which you want to delete a profile.

5 Click the **Service Profiles** tab.

6 Click the profile that you want to delete.

7 Click the **Delete** icon ( ).

11 vShield App Management

vShield App is a hypervisor-based firewall that protects applications in the virtual datacenter from network-based attacks. Organizations gain visibility and control over network communications between virtual machines. You can create access control policies based on logical constructs such as VMware vCenter™ containers and vShield security groups—not just physical constructs such as IP addresses. In addition, flexible IP addressing offers the ability to use the same IP address in multiple tenant zones to simplify provisioning.

You should install vShield App on each ESX host within a cluster so that VMware vMotion operations work and virtual machines remain protected as they migrate between ESX hosts. By default, a vShield App virtual appliance cannot be moved by using vMotion.

NOTE vShield App does not support FT enabled virtual machines.

This chapter includes the following topics:

- "Sending vShield App System Events to a Syslog Server," on page 157
- "Viewing the Current System Status of a vShield App," on page 158
- "Restart a vShield App," on page 158
- "Forcing a vShield App to Synchronize with the vShield Manager," on page 158
- "Viewing Traffic Statistics by vShield App Interface," on page 159
- "Download Technical Support Logs for vShield App," on page 159
- "Configuring Fail Safe Mode for vShield App Firewall," on page 159
- "Excluding Virtual Machines from vShield App Protection," on page 159

Sending vShield App System Events to a Syslog Server

You can send vShield App system messages related to firewall events that flow from vShield App appliances to a syslog server.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 Click the **vShield** tab.

4 In the **Service Virtual Machines** area, expand the vShield App SVM.

5 In the Syslog Servers area, type the IP address of the syslog server.

6 From the **Log Level** drop-down menu, select the event level at and above which to send vShield App events to the syslog server.

For example, if you select **Emergency**, then only emergency-level events are sent to the syslog server. If you select **Critical**, then critical-, alert-, and emergency-level events are sent to the syslog server.

You send vShield App events to up to three syslog instances.

7 Click **Save** to save the new settings.

Viewing the Current System Status of a vShield App

The **System Status** option lets you view and influence the health of a vShield App. Details include system statistics, status of interfaces, software version, and environmental variables.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 Click the **vShield** tab.

4 In the **Service Virtual Machines** area, expand the vShield App SVM.

The Resource Utilization panel displays the system details for the vShield App.

Restart a vShield App

You can restart a vShield App to troubleshoot an operational issue.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 Click the **vShield** tab.

4 In the **Service Virtual Machines** area, expand the vShield App SVM.

5 Click **Restart**.

Forcing a vShield App to Synchronize with the vShield Manager

The **Force Sync** option forces a vShield App to re-synchronize with the vShield Manager. This might be necessary after a software upgrade.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 Click the **vShield** tab.

4 In the **Service Virtual Machines** area, expand the vShield App SVM.

5 Click **Force Sync**.

Viewing Traffic Statistics by vShield App Interface

You can view the traffic statistics for each vShield interface.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 Click the **vShield** tab.

4 In the **Service Virtual Machines** area, expand the vShield App SVM.

The Management Port Interface panel displays the traffic statistics for the vShield App.

Download Technical Support Logs for vShield App

You can download technical support logs for each host on which you have installed vShield App.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a host from the resource tree.

3 In Service Virtual Machines, click **Download Support logs**.

4 Click **Log file generated; click here to download**.

5 Open or save the log file.

Configuring Fail Safe Mode for vShield App Firewall

By default, traffic is blocked when the vShield App appliance fails or is unavailable. You can change the fail safe mode to allow traffic to pass.

Procedure

1 Log in to the vShield Manager.

2 Click **Settings & Reports** from the vShield Manager inventory panel.

3 Click the **vShield App** tab.

4 In **Fail Safe**, click **Change**.

5 In Change App Fail Policy, click **Yes**.

Excluding Virtual Machines from vShield App Protection

You can exclude a set of virtual machines from vShield App protection. This exclusion list is applied across all vShield App installations within the specified vShield Manager. If a virtual machine has multiple vNICs, all of them are excluded from protection.

The vShield Manager and service virtual machines are automatically excluded from vShield App protection. You should exclude the vCenter server and partner service virtual machines as well to allow traffic to flow freely.

Excluding virtual machines from vShield App protection is useful for instances where vCenter Server resides in the same cluster where vShield App is being utilized. After enabling this feature, no traffic from excluded virtual machines will go through the vShield App appliance.

NOTE vCenter Server can be moved to a cluster that is protected by vShield App, but it must already exist in the exclusion list to avoid any connection issues to vCenter Server.

Procedure

1 Log in to the vShield Manager.

2 Click **Settings & Reports** from the vShield Manager inventory panel.

3 Click the **App Global Configuration** tab.

4 In **Virtual Machines Exclusion List**, click **Add.**

The Add Virtual Machines to Exclude dialog box opens.

5 Click in the field next to Select and click the virtual machine you want to exclude.

6 Click **Select.**

The selected virtual machine is added to the list.

7 Click **OK**.

vShield App Flow Monitoring 12

Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic on your virtual network that passed through a vShield App. The Flow Monitoring output defines which machines are exchanging data and over which application. This data includes the number of sessions, packets, and bytes transmitted per session. Session details include sources, destinations, direction of sessions, applications, and ports being used. Session details can be used to create firewall allow or block rules.

You can use Flow Monitoring as a forensic tool to detect rogue services and examine outbound sessions.

This chapter includes the following topics:

- "Viewing the Flow Monitoring Data," on page 161
- "Add or Edit App Firewall Rule from the Flow Monitoring Report," on page 164
- "Change the Date Range of the Flow Monitoring Charts," on page 165

Viewing the Flow Monitoring Data

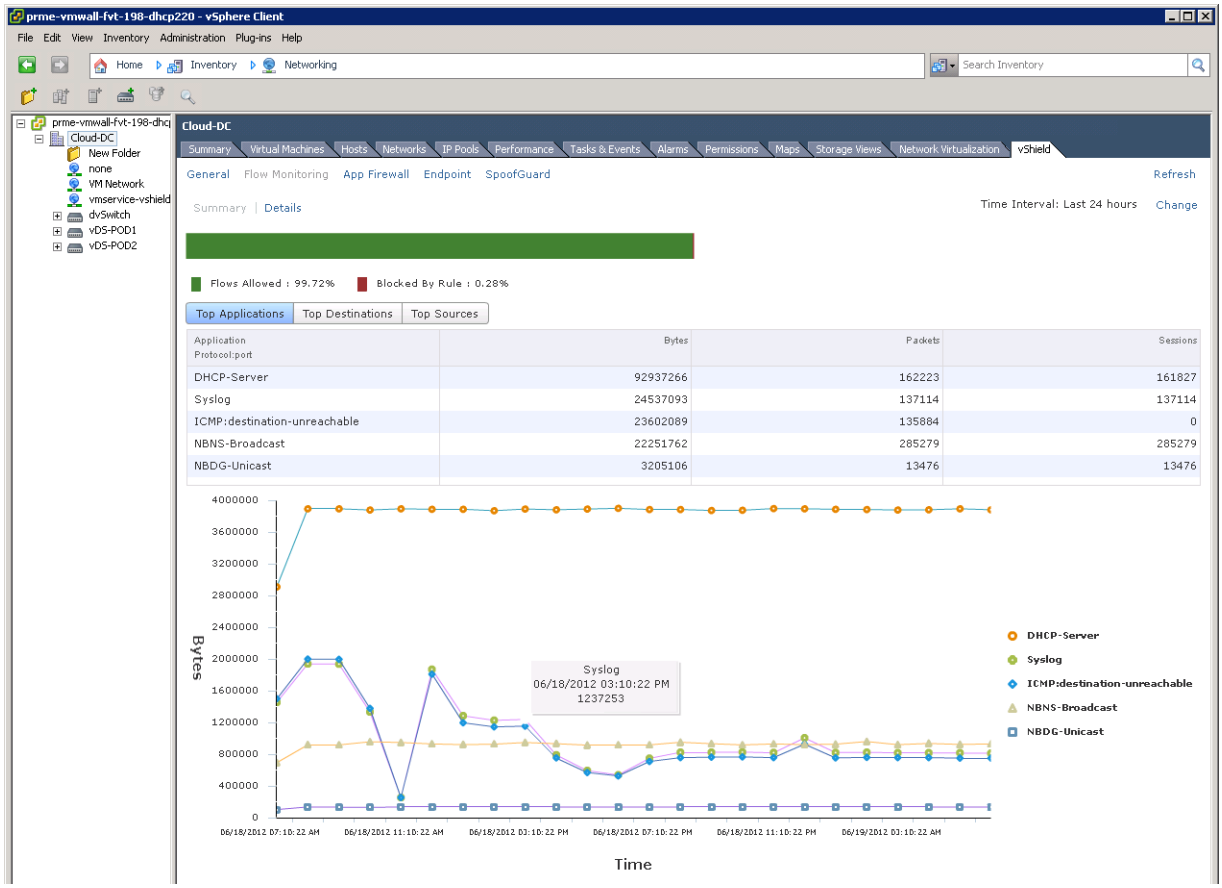
You can view traffic sessions inspected by a vShield App within the specified time span. The last 24 hours of data are displayed by default, the minimum time span is one hour and the maximum is two weeks.

Procedure

1 In the vSphere Client, select a datacenter, virtual machine, port group, network adapter, or virtual wire.

Option	Action
Select a datacenter or virtual machine	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter or virtual machine. c Click the **vShield** tab.
Select a port group or network adapter	a Go to **Inventory > Networking**. b Select a port group or network adapter. c Click the **vShield** tab.
Select a virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. NOTE The Flow Monitoring tab for a virtual wire is available only if vShield App is installed on at least one of the hosts in the cluster from which the virtual wire has been created. Flow monitoring data is displayed only for the traffic passing through the host which has vShield App installed on it.

2 Click **Flow Monitoring**.



The charts update to display the most current information for the last twenty four hours. This might take several seconds.

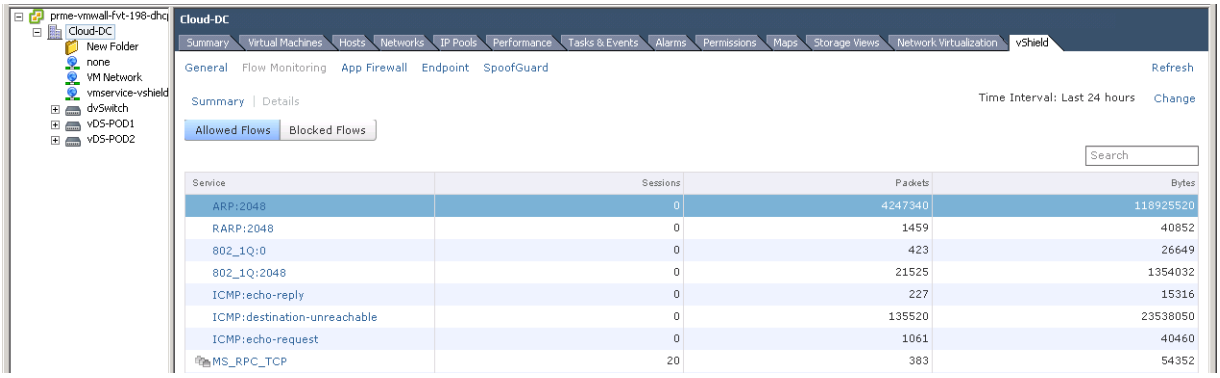
The bar on the top of the page shows the percentage of allowed traffic in green, blocked traffic in red, and traffic blocked by SpoofGuard in orange.

Traffic statistics are displayed in three tabs:

- **Top Flows** displays the total incoming and outgoing traffic per service over the specified time period. The top five services are displayed.
- **Top Destinations** displays incoming traffic per destination over the specified time period. The top five destinations are displayed.
- **Top Sources** displays outgoing traffic per source over the specified time period. The top five sources are displayed.

Each tab displays traffic information in a line graph. Moving the mouse over plot points on the graph displays the application/protocol:port, traffic source, or destination depending on the tab selected, date and time that the traffic passed through vShield App, and the packet size.

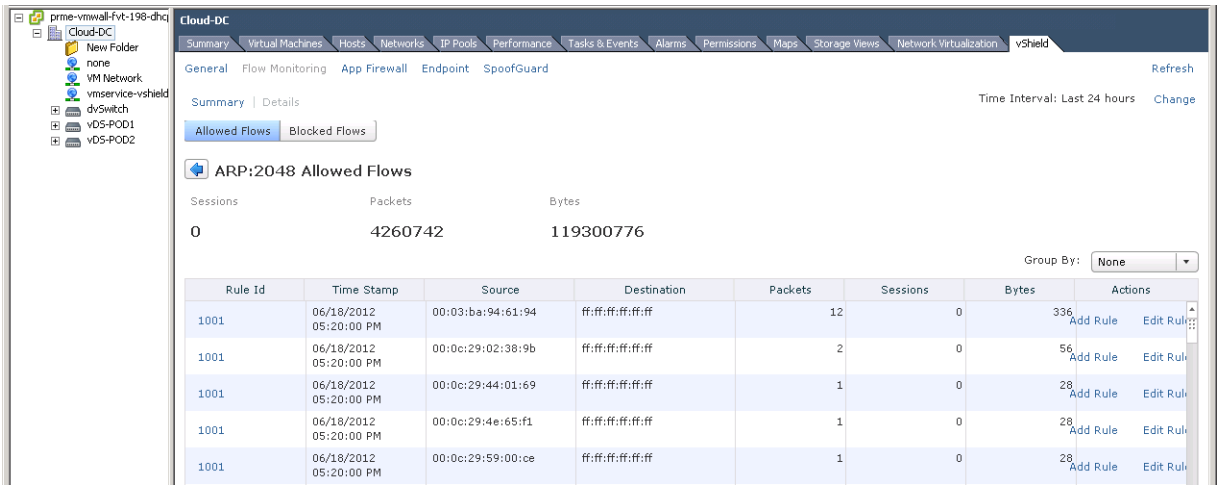
3 Click the **Details** tab.



Details about all traffic for the selected service is displayed. Click **Load More Records** to display additional flows. The **Allowed Flows** tab displays the allowed traffic sessions and the **Blocked Flows** tab displays the blocked traffic.

You can search on service names.

4 Click an item in the table to display the rules that allowed or blocked that traffic flow.



The Description column indicates whether this traffic has been blocked by a rule or by spoofguard.Click **Load More Records** to display additional flows.

5 To group rules, select the appropriate option in the **Group By** drop-down.

6 Click the **Rule Id** for a rule to display the rule details.

Add or Edit App Firewall Rule from the Flow Monitoring Report

By drilling down into the traffic data, you can evaluate the use of your resources and send session information to App Firewall to create a new allow or block rule at any level.

Procedure

1 In the vSphere Client, select a datacenter, virtual machine, port group, network adapter, or virtual wire.

Option	Action
Select a datacenter or virtual machine	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter or virtual machine. c Click the **vShield** tab.
Select a port group or network adapter	a Go to **Inventory > Networking**. b Select a port group or network adapter. c Click the **vShield** tab.
Select a virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. NOTE The Flow Monitoring tab for a virtual wire is available only if vShield App is installed on at least one of the hosts in the cluster from which the virtual wire has been created. Flow monitoring data is displayed only for the traffic passing through the host which has vShield App installed on it.

2 Click **Flow Monitoring**.

The charts update to display the most current information for the last twenty four hours. This might take several seconds.

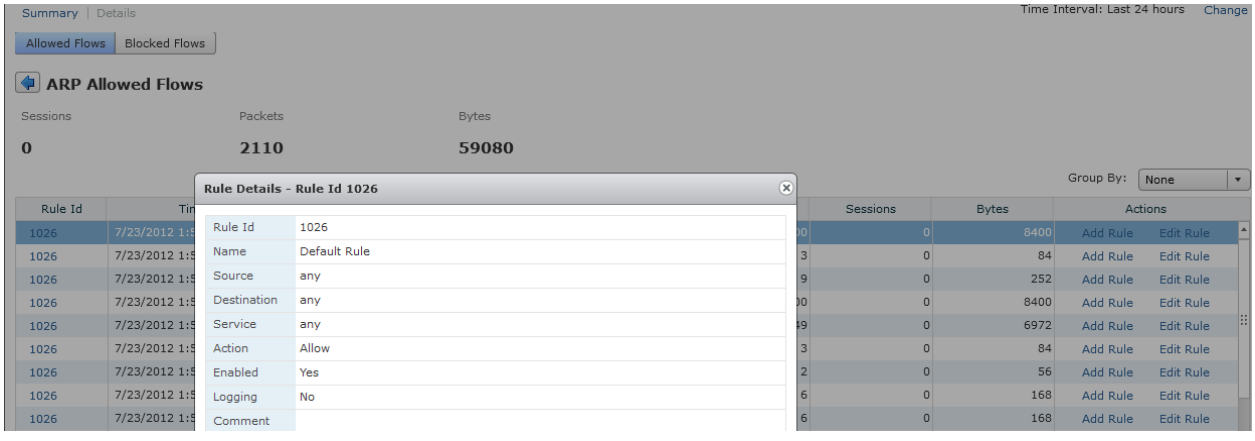
3 Click the **Details** tab.

Click **Load More Records** to display additional flows.

4 Click a service to view the traffic flow for it.

All rules that allowed or denied traffic for this service are displayed.

5 Click a rule ID to view rule details.



6 Do one of the following:

- To edit a rule:
  1 Click **Edit Rule** in the **Actions** column.
  2 Change the name, action, or comments for the rule.
  3 Click OK.
- To add a rule:
  1 Click **Add Rule** in the **Actions** column.
  2 Complete the form to add a rule.

  You cannot add a protocol, IP address, or MAC address as the source or destination for a firewall rule. If the source or destination for the rule is an IP or MAC address, you must create an IPSet or MACSet for that address. If the source or destination for the rule is a protocol, you must create a service for that address.

  For information on completing the firewall rule form, see "Add a Firewall Rule," on page 169.
  3 Click **OK**.

  The rule is added at the top of the firewall rule table.

Change the Date Range of the Flow Monitoring Charts

You can change the date range of the flow monitoring data for an historical view of traffic data.

Procedure

1 In the vSphere Client, select a datacenter, virtual machine, port group, network adapter, or virtual wire.

Option	Action
Select a datacenter or virtual machine	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter or virtual machine. c Click the **vShield** tab.
Select a port group or network adapter	a Go to **Inventory > Networking**. b Select a port group or network adapter. c Click the **vShield** tab.
Select a virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab. NOTE The Flow Monitoring tab for a virtual wire is available only if vShield App is installed on at least one of the hosts in the cluster from which the virtual wire has been created. Flow monitoring data is displayed only for the traffic passing through the host which has vShield App installed on it.

2 Click **Flow Monitoring**.

The charts update to display the most current information for the last twenty four hours. This might take several seconds.

3 Next to **Time Period**, click **Change**.

4 Select the time period or type a new start and end date.

The maximum time span for which you can view traffic flow data is the previous two weeks.

5 Click **Update**.

vShield App Firewall Management 13

vShield App provides firewall protection through access policy enforcement. The App Firewall tab represents the vShield App firewall access control list.

This chapter includes the following topics:

- "Using App Firewall," on page 167
- "Working with Firewall Rules," on page 169
- "Using SpoofGuard," on page 174

Using App Firewall

The App Firewall service is a centralized firewall for ESX hosts. App Firewall enables you to create rules that allow or block access to and from your virtual machines. Each installed vShield App enforces the App Firewall rules.

You can manage App Firewall rules on a namespace level to provide a consistent set of rules across multiple vShield App instances under these containers. Namespace levels include datacenter, virtual wire, and port group with an independent namespace. As membership in these containers can change dynamically, App Firewall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, App Firewall effectively has a continuous footprint on each ESX host under the managed containers.

Namespaces in a Multi Tenant Environment

The namespace feature allows vShield App to work in a multi tenant mode. Each tenant can have its own firewall rules and security groups.

By default, all port groups in a datacenter share the same IP space. You can assign an independent namespace to a port group, and then the datacenter level firewall rules no longer apply to that port group.

To assign an independent IP address to a port group

1 In the vSphere Client, go to **Inventory > Networking.**

2 Select a port group from the resource tree.

3 Click the **vShield** tab.

4 Click **Namespace.**

5 Click **Change to Independent namespace**.

6 Click **Reload** to view the updated information.

About Services and Service Groups

A service is a protocol-port combination and a service group is a combination of two or more services. You can define firewall rules for services and service groups

For information on creating applications, see "Working with Services and Service Groups," on page 27.

Designing Security Groups

When creating App Firewall rules, you can create rules based on traffic to or from a specific container that encompasses all of the resources within that container. For example, you can create a rule to block any traffic from inside of a cluster that targets a specific destination outside of the cluster. You can create a rule to block any incoming traffic that is not tagged with a VLAN ID. When you specify a container as the source or destination, all IP addresses within that container are included in the rule.

A security group is a trust zone that you create and assign resources to for App Firewall protection. Security groups are containers, like a vApp or a cluster. Security groups enables you to create a container by assigning resources arbitrarily, such as virtual machines and network adapters. After the security group is defined, you add the group as a container in the source or destination field of an App Firewall rule. For more information, see "Grouping Objects," on page 30.

The security group scope is limited to the resource level at which it is created. For example, if you create a security group at a datacenter level, the security group is available to be added as a source or destination only when you create a firewall rule at the datacenter level. If you create a rule for a port group with an independent namespace within that datacenter, the security group is not available.

About System Defined Rules in App Firewall

The default App Firewall rule allows all traffic to pass through all vShield App instances. The default rule for L3 traffic appears in the firewall table in the **General** tab, and the default rule for L2 traffic appears in the firewall table in the **Ethernet** tab. The default rule is always at the bottom of the rules table and cannot be deleted or added to. However, you can change the **Action** element of each rule from **Allow** to **Block**, comments for the rule, and whether traffic for that rule should be logged.

About General and Ethernet Rules

The **App Firewall** tab offers multiple sets of configurable rules: Layer 3 (L3) rules (**General** tab) and Layer 2 (L2) rules (**Ethernet** tab).

By default, all general and ethernet traffic is allowed to pass. You can configure rules at the datacenter, virtual wire, and port group with independent namespace levels.

Firewall Rules Precedence

Each vShield App enforces App Firewall rules in top-to-bottom ordering. A vShield App checks each traffic session against the top rule in the App Firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced.

Ethernet rules are enforced before general rules.

Planning App Firewall Rule Enforcement

Using App Firewall, you can configure allow and block rules based on your network policy.

The following examples represent two common firewall policies:

Allow all traffic by default	You keep the default allow all rules and add block rules based on Flow Monitoring data or manual App Firewall rule configuration. In this scenario, if a session does not match any of the block rules, vShield App allows the traffic to pass.
Block all traffic by default	You can change the **Action** status of the default rules from **Allow** to **Block**, and add allow rules explicitly for specific systems and applications. In this scenario, if a session does not match any of the allow rules, vShield App drops the session before it reaches its destination. If you change all of the default rules to block any traffic, vShield App drops all incoming and outgoing traffic.

Working with Firewall Rules

You can configure and publish L3 and L2 firewall rules before or after installing an application. Once an application is installed, the last published firewall rules are applied.

Add a Firewall Rule

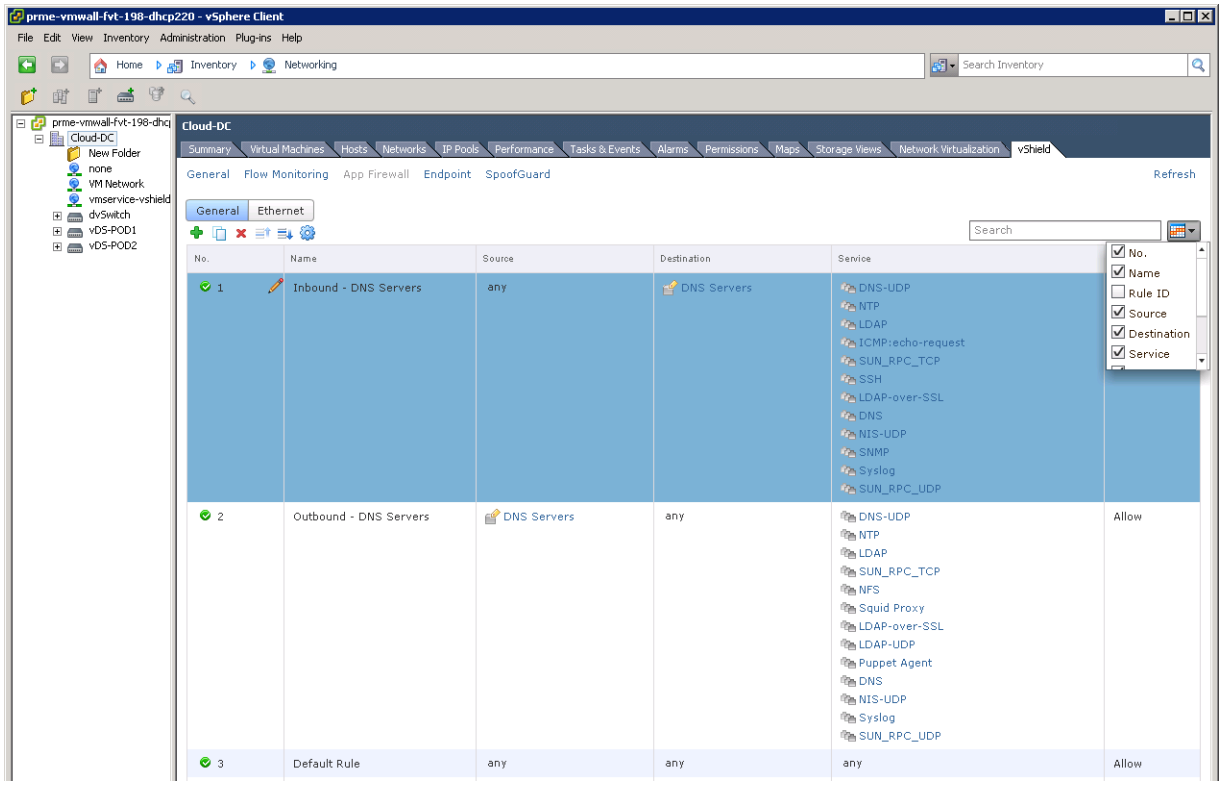
You can add a firewall rule at various container (datacenter, virtual wire, port group with independent namespace) levels. Adding multiple objects per rule at the source and destination levels helps you reduce the total number of firewall rules to be created.

Procedure

1 In the vSphere Client, select a datacenter, virtual wire, or port group with an independent namespace.

Firewall Rule Level	Method
Datacenter	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab.
Port group with an independent namespace	a Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab.

2 Click the **App Firewall** tab. For a virtual wire, ensure that you are in the **Firewall** tab.


prme-vmwall-fvt-198-dhcp220 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Networking
Search Inventory
Cloud-DC
Summary Virtual Machines Hosts Networks IP Pools Performance Tasks & Events Alarms Permissions Maps Storage Views Network Virtualization vShield
General Flow Monitoring App Firewall Endpoint SpoofGuard
Refresh
General Ethernet
Search
No. Name Source Destination Service
1 Inbound - DNS Servers any DNS Servers DNS-UDP NTP LDAP ICMP:echo-request SUN_RPC_TCP SSH LDAP-over-SSL DNS NIS-UDP SNMP Syslog SUN_RPC_UDP
2 Outbound - DNS Servers DNS Servers any DNS-UDP NTP LDAP SUN_RPC_TCP NFS Squid Proxy LDAP-over-SSL LDAP-UDP Puppet Agent DNS NIS-UDP Syslog SUN_RPC_UDP Allow
3 Default Rule any any any Allow
No.
Name
Rule ID
Source
Destination
Service

3 Ensure that you are in the **General** tab to add an L3 rule. click the **Ethernet** tab to add an L2 rule.

4 Do one of the following.

- To add a rule at a specific place in the firewall table, follow the steps below.
  a Select a rule.
  b In the No. column, click ⊞ and select **Add Above** or **Add Below**.
- To add a rule by copying a rule, follow the steps below.
  a Select a rule.
  b Click the Copy ( ) icon.
  c Select a rule.
  d In the No. column, click ⊞ and select **Paste Above** or **Paste Below**.

◆ Click the **Add** ( ) icon.

A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.

5 Point to the **Name** cell of the new rule and click ⊞.

6 Type a name for the new rule.

7 Point to the **Source** cell of the new rule and click ⊞.

a In **View**, select a container from which the communication originated.

Objects for the selected container are displayed.

b Select one or more objects and click .

You can create a new security group or IPSet. Once you create the new object, it is added to the source column by default. For information on creating a new security group or IPSet, see "Grouping Objects," on page 30.

c To specify a source port, click **Advance options** and type the port number or range.

d Select **Negate Source** to exclude this source port from the rule.

Option	Result
Negate Source selected	Rule applied to traffic coming from all sources except for the source you specified in Step 7c.
Negate Source not selected	Rule applies to traffic coming from the source you specified in Step 7c.

e Click **OK**.

8 Point to the **Destination** cell of the new rule and click ⊞.

a In **View**, select a container which the communication is targeting.

Objects for the selected container are displayed.

b Select one or more objects and click .

You can create a new security group or IPSet. Once you create the new object, it is added to the destination column by default. For information on creating a new security group or IPSet, see "Grouping Objects," on page 30.

c To specify a destination port, click **Advance options** and type the port number or range.

d Select **Negate Destination** to exclude this destination port from the rule.

Option	Rule Applied To
Negate Destination selected	Traffic going to all destinations except for the destination you specified in Step 8c.
Negate Destination not selected	Traffic going to the destination you specified in Step 8c.

e Click **OK**.

9 Point to the **Action** cell of the new rule and click ⊞.

a Click **Block** to block traffic from or to the specified source and destination.

b Click **Log** to log all sessions matching this rule.

Enabling logging can affect performance.

c Type comments if required.

d Click **OK**.

10 Click **Publish Changes** to push the new rule to all vShield App instances.

What to do next

- Disable a rule by clicking or enable a rule by clicking .
- Display additional columns in the rule table by clicking and selecting the appropriate columns.

Column Name	Information Displayed
Rule ID	Unique system generated ID for each rule
Log	Traffic for this rule is being logged or not
Stats	Clicking shows the traffic affected by this rule (number of sessions, traffic packets, and size)
Comments	Comments for the rule

- Search for rules by typing text in the Search field.

Delete a Firewall Rule

You can delete firewall rules that you created, but not the default rule.

Procedure

1 Do one of the following.

Firewall Rule Level	Method
Datacenter	a In the vSphere client, Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab. d Click the **App Firewall** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab. e Ensure that you are in the **Firewall** tab.
Port group with an independent namespace	a In the vSphere client, Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab. d Click the **App Firewall** tab.

2 Click a rule.

3 Click **Delete Rule** ( ).

Revert to a Previous Firewall Configuration

The vShield Manager saves the App firewall settings each time you publish a new rule. Clicking **Publish Changes** causes the vShield Manager to save the previous configuration with a timestamp before adding the new rule. These configurations are available from the **History** drop-down list. vShield Manager saves the previous ten configurations.

Procedure

1 Do one of the following.

Firewall Rule Level	Method
Datacenter	a In the vSphere client, Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab. d Click the **App Firewall** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab. e Ensure that you are in the **Firewall** tab.
Port group with an independent namespace	a In the vSphere client, Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab. d Click the **App Firewall** tab.

2 Click **History Options** ( ) and select **Load History**.

The Load History dialog box displays the previous configurations in the order of timestamps, with the most recent configuration listed at the top.

3 Select the configuration to which you want to revert.

4 Click **OK**.

5 In the Load Configuration dialog box, click **OK**.

6 Click **Publish Changes**.

The selected configuration is loaded.

Change the Order of a Rule

Firewall rules are applied in the order in which they exist in the rule table. You can move a custom rule up or down in the table - the default rule is always at the bottom of the table and cannot be moved.

Procedure

1 Do one of the following.

Firewall Rule Level	Method
Datacenter	a In the vSphere client, Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab. d Click the **App Firewall** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab. e Ensure that you are in the **Firewall** tab.
Port group with an independent namespace	a In the vSphere client, Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab. d Click the **App Firewall** tab.

2 Select the rule that you want to move.

3 Click the **Move rule up** ( ) or **Move rule down** ( ) icon.

4 Click **Publish Changes**.

Using SpoofGuard

After synchronizing with the vCenter Server, the vShield Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. Up to vShield 4.1, vShield trusted the IP address provided by VMware Tools on a virtual machine. However, if a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

SpoofGuard allows you to authorize the IP addresses reported by VMware Tools, and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from the App Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed. A SpoofGuard policy supports a single IP address to vNIC assignment. IPv6 is not supported.

When enabled, you can use SpoofGuard to monitor and manage the IP addresses reported by your virtual machines in one of the following modes.

Automatically Trust IP Assignments On Their First Use	This mode allows all traffic from your virtual machines to pass while building a table of vnic-to-IP address assignments. You can review this table at your convenience and make IP address changes.
Manually Inspect and Approve All IP Assignments Before Use	This mode blocks all traffic until you approve each MAC-to-IP address assignment.

NOTE SpoofGuard inherently allows DHCP requests regardless of enabled mode. However, if in manual inspection mode, traffic does not pass until the DHCP-assigned IP address has been approved.

SpoofGuard Screen Options

The SpoofGuard interface contains the following options.

Table 13-1. SpoofGuard Screen Options

Option	Description
Active Virtual NICs	List of all validated IP addresses
Active Virtual NICs Since Last Published	List of IP addresses that have been validated since the policy was last updated
Virtual NICs IP Required Approval	IP address changes that require approval before traffic can flow to or from these virtual machines
Virtual NICs with Duplicate IP	IP addresses that are duplicates of an existing assigned IP address within the selected datacenter
Inactive Virtual NICs	List of IP addresses where the current IP address does not match the published IP address
Unpublished Virtual NICs IP	List of virtual machines for which you have edited the IP address assignment but have not yet published

Enable SpoofGuard

Once enabled, you can use SpoofGuard to manage IP address assignments for your entire vCenter inventory.

IMPORTANT You must upgrade all vShield App instances to vShield App 1.0.0 Update 1 or later before you enable SpoofGuard.

Procedure

1 In the vSphere Client, select a datacenter, virtual wire, or port group with an independent namespace.

SpoofGuard Scope	Method
Datacenter	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab.
Port group with an independent namespace	a Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab.

2 Click the **SpoofGuard** tab.

3 Click **Edit** at the right side of the SpoofGuard window.

4 For **SpoofGuard**, click **Enable**.

5 For **Operation Mode**, select one of the following:

Option	Description
Automatically Trust IP Assignments on Their First Use	Select this option to trust all IP assignments upon initial registration with the vShield Manager.
Manually Inspect and Approve All IP Assignments Before Use	Select this option to require manual approval of all IP addresses. All traffic to and from unapproved IP addresses is blocked.

6 Click **Allow local address as valid address in this namespace** to allow local IP addresses in your setup.

When you power on a virtual machine but it is unable to connect to the DHCP server, a local IP address is assigned to it. This local IP address is considered valid only if the SpoofGuard mode is set to **Allow local address as valid address in this namespace**. Otherwise, the local IP address is ignored.

7 Click **OK**.

Approve IP Addresses

If you set SpoofGuard to require manual approval of all IP address assignments, you must approve IP address assignments to allow traffic from those virtual machines to pass.

Procedure

1 In the vSphere Client, select a datacenter, virtual wire, or port group with an independent namespace.

Firewall Rule Level	Method
Datacenter	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab.
Port group with an independent namespace	a Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab.

2 Click the **SpoofGuard** tab.

3 Click one of the option links.

4 Select the virtual NIC for which you want to approve the IP address.

5 Click **Approve Detected IP**.

6 Click **Publish Now**.

Edit an IP Address

You can edit the IP address assigned to a MAC address to correct the assigned IP address.

NOTE SpoofGuard accepts a unique IP address from virtual machines. However, you can assign an IP address only once. An approved IP address is unique across the vShield system. Duplicate approved IP addresses are not allowed.

Procedure

1 In the vSphere Client, select a datacenter, virtual wire, or port group with an independent namespace.

Firewall Rule Level	Method
Datacenter	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab.
Port group with an independent namespace	a Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab.

2 Click the **SpoofGuard** tab.

3 Click the **Virtual NICs IP Required Approval** or **Virtual NICs with Duplicate IP** link.

4 Point to the Approved IP cell and click .

5 Type the new IP address.

6 Click **OK**.

7 Click **Publish Now**.

Delete an IP Address

You can delete a MAC-to-IP address assignment from the SpoofGuard table to clean the table of a virtual machine that is no longer active. Any deleted instance can reappear in the SpoofGuard table based on viewed traffic and the current enabled state of SpoofGuard.

Procedure

1 In the vSphere Client, select a datacenter, virtual wire, or port group with an independent namespace.

Firewall Rule Level	Method
Datacenter	a Go to **Inventory > Hosts and Clusters**. b Select a datacenter. c Click the **vShield** tab.
Virtual wire	a Go to **Inventory > Hosts and Clusters** and select the **Network Virtualization** tab. b Click the Networks tab. c In the **Name** column, click the virtual wire for which you want to add a rule. d Click the **Security** tab.
Port group with an independent namespace	a Go to **Inventory > Networking**. b Select a Port group with an independent namespace. c Click the **vShield** tab.

2 Click the **SpoofGuard** tab.

3 Click one of the option links.

4 Click **Clear Approved IP**.

5 Click **Publish Now**.

vShield Endpoint Events and Alarms 14

vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn't go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

vShield Endpoint health status is conveyed by using alarms that show in red on the vCenter Server console. In addition, more status information can be gathered by looking at the event logs.

IMPORTANT Your vCenter Server must be correctly configured for vShield Endpoint security:

- Not all guest operating systems are supported by vShield Endpoint. Virtual machines with non-supported operating systems are not protected by the security solution. For information on the supported operating systems, see the Installing vShield Endpoint section in the *vShield Quick Start Guide*.
- All hosts in a resource pool containing protected virtual machines must be prepared for vShield Endpoint so that virtual machines continue to be protected as they are vMotioned from one ESX host to another within the resource pool.

This chapter includes the following topics:

- "View vShield Endpoint Status," on page 179
- "vShield Endpoint Alarms," on page 180
- "vShield Endpoint Events," on page 180
- "vShield Endpoint Audit Messages," on page 181

View vShield Endpoint Status

Monitoring a vShield Endpoint instance involves checking for status coming from the vShield Endpoint components: the security virtual machine (SVM), the ESX host-resident vShield Endpoint module, and the protected virtual machine-resident thin agent.

Procedure

1. In the vSphere Client, go to **Inventory > Hosts and Clusters**.
2. Select a datacenter, cluster, or ESX host resource from the resource tree.
3. Click the **vShield** tab.

4 Click **Endpoint**.

The vShield Endpoint Health and Alarms page displays the health of the objects under the datacenter, cluster, or ESX host you selected, and the active alarms. Health status changes are reflected within a minute of the actual occurrence of the event that triggered the change.

vShield Endpoint Alarms

Alarms signal the vCenter Server administrator about vShield Endpoint events that require attention. Alarms are automatically cancelled in case the alarm state is no longer present.

vCenter Server alarms can be displayed without a custom vSphere plug-in. See the *vCenter Server Administration Guide* on events and alarms.

Upon registering as a vCenter Server extension, the vShield Manager defines the rules that create and remove alarms, based on events coming from the three vShield Endpoint components: SVM, vShield Endpoint module, and thin agent. Rules can be customized. For instructions on how to create new custom rules for alarms, see the vCenter Server documentation. In some cases, there are multiple possible causes for the alarm. The tables that follow list the possible causes and the corresponding actions you might want to take for remediation.

Host Alarms

Host alarms are generated by events affecting the health status of the vShield Endpoint module.

Table 14-1. Errors (Marked Red)

Possible Cause	Action
The vShield Endpoint module has been installed on the host, but is no longer reporting status to the vShield Manager.	1 Ensure that vShield Endpoint is running by logging in to the host and typing the command `/etc/init.d/vShield-Endpoint-Mux start` 2 Ensure that the network is configured properly so that vShield Endpoint can connect to the vShield Manager. 3 Reboot the vShield Manager.

SVM Alarms

SVM alarms are generated by events affecting the health status of the SVM.

Table 14-2. Red SVM Alarms

Problem	Action
There is a protocol version mismatch with the vShield Endpoint module	Ensure that the vShield Endpoint module and SVM have a protocol that is compatible with each other.
vShield Endpoint could not establish a connection to the SVM	Ensure that the SVM is powered on and that the network is configured properly.
The SVM is not reporting its status even though guests are connected.	Internal error. Contact your VMware support representative.

vShield Endpoint Events

Events are used for logging and auditing conditions inside the vShield Endpoint-based security system.

Events can be displayed without a custom vSphere plug-in. See the *vCenter Server Administration Guide* on events and alarms.

Events are the basis for alarms that are generated. Upon registering as a vCenter Server extension, the vShield Manager defines the rules that create and remove alarms.

Common arguments for all events are the event time stamp and the vShield Manager `event_id`.

The following table lists vShield Endpoint events reported by the SVM and the vShield Manager (VSM).

Table 14-3. vShield Endpoint Events

Description	Severity	VC Arguments
vShield Endpoint solution *SolutionName* enabled. Supporting version *versionNumber* of the VFile protocol.	info	timestamp
ESX module enabled.	info	timestamp
ESX module uninstalled.	info	timestamp
The vShield Manager has lost connection with the ESX module.	info	timestamp
vShield Endpoint solution *SolutionName* was contacted by a non-compatible version of the ESX module.	error	timestamp, solution version, ESX module version
A connection between the ESX module and *SolutionName* failed.	error	timestamp, ESX module version, solution version
vShield Endpoint failed to connect to the SVM.	error	timestamp
vShield Endpoint lost connection with the SVM.	error	timestamp

vShield Endpoint Audit Messages

Audit messages include fatal errors and other important audit messages and are logged to `vmware.log`.

The following conditions are logged as AUDIT messages:

- Thin agent initialization success (and version number.)
- Thin agent initialization failure.
- Established first time communication with SVM.
- Failure to establish communication with SVM (when first such failure occurs).

Generated log messages have the following substrings near the beginning of each log message: `vf–AUDIT`, `vf–ERROR`, `vf–WARN`, `vf–INFO`, `vf–DEBUG`.

vShield Data Security Management 15

vShield Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by vShield Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

To begin using vShield Data Security, you create a policy that defines the regulations that apply to data security in your organization and specifies the areas of your environment and files to be scanned. A regulation is composed of content blades, which identify the sensitive content to be detected. vShield supports PCI, PHI, and PII related regulations only.

When you start a Data Security scan, vShield analyzes the data on the virtual machines in your vSphere inventory and reports the number of violations detected and the files that violated your policy.

You can perform all data security tasks using REST APIs. For more information, see the vShield API Programming Guide.

This chapter includes the following topics:

- "vShield Data Security User Roles," on page 183
- "Defining a Data Security Policy," on page 184
- "Editing a Data Security Policy," on page 186
- "Running a Data Security Scan," on page 187
- "Viewing and Downloading Reports," on page 187
- "Creating Regular Expressions," on page 188
- "Available Regulations," on page 188
- "Available Content Blades," on page 204
- "Supported File Formats," on page 223

vShield Data Security User Roles

A user's role determines the actions that the user can perform.

Role	Actions Allowed
Security Administrator	Create and publish policies and view violation reports. Cannot start or stop a data security scan.
vShield Administrator	Start and stop data security scans.
Auditor	View configured policies and violation reports.

Defining a Data Security Policy

To detect sensitive data in your environment, you must create a data security policy. You must be a Security Administrator to create policies.

To define a policy, you must specify the following:

1 Regulations

A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information. You can select the regulations that your company needs to comply to. When you run a scan, vShield Data Security identifies data that violates the regulations in your policy and is sensitive for your organization.

2 Participating Areas

By default, your entire vSphere infrastructure is scanned by vShield Data Security. To scan a subset of the inventory, you can exclude or include security groups. If a resource (cluster, datacenter or host) is part of both an excluded and included security group, the exclude list takes precedence and the resource is not scanned.

3 File filters

You can create filters to limit the data being scanned and exclude file types unlikely to contain sensitive data from the scan.

Select Regulations

Once you select the regulations that you want your company data to comply with, vShield can identify files that contain information which violates these particular regulations.

Prerequisites

You must have been assigned the Security Administrator role.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a datacenter.

NOTE Even though you are selecting a datacenter, the policy that you configure will be applied to the entire vSphere inventory.

3 Click the **vShield** tab and click **Data Security**.

4 Click the **Policy** tab and expand **Regulations and standards to detect**.

5 Click **Edit** and click **All** to display all available regulations.

6 Select the regulations for which you want to detect compliance.

NOTE For information on available regulations, see "Available Regulations," on page 188.

7 Click **Next.**

8 Certain regulations require additional information for vShield Data Security to recognize sensitive data. If you selected a regulation that monitors Group Insurance Numbers, Patient Identification Numbers, Medical Record Numbers, Health Plan Beneficiary Numbers, US Bank Account Numbers, Custom Accounts, or Student identification numbers, specify a regular expression pattern for identifying that data.

NOTE Check the accuracy of the regular expression. Specifying incorrect regular expressions can slow down the discovery process. For more information on regular expressions, see "Creating Regular Expressions," on page 188.

9 Click **Finish.**

10 If you are updating an existing policy, click **Publish Changes** to apply it.

Specify Areas Participating in the Policy Scan

By default, your entire vSphere infrastructure is scanned by vShield Data Security. To scan a subset of the inventory, you can exclude or include security groups. If a resource (cluster, datacenter or virtual machine) is part of both an excluded and included security group, the exclude list takes precedence and the resource is not scanned.

vShield special appliances (such as vShield Endpoint and Shield App appliances as well as partner appliances that leverage vShield Endpoint) are not scanned by vShield Data Security

Prerequisites

You must have been assigned the Security Administrator role.

Procedure

1 In the Policy tab of the Data Security panel, expand **Participating Areas**.

2 To include a security group in the data security scan, click **Change** next to **Scan the following infrastructure**.

   a In the Include Security Groups dialog box, type the name of the security group to be included in the scan.

   b Click **Add**.

   c Click **Save**.

3 To exclude an existing security group from the data security scan, click **Change** next to **Except for the following areas**.

   a In the Exclude Security Groups dialog box, type the name of the security group to be excluded from the scan.

   b Click **Add**.

   c Click **Save**.

4 If you are updating an existing policy, click **Publish Changes** to apply it.

Specify File Filters

You can restrict the files that you want to monitor based on size, last modified date, or file extensions.

Prerequisites

You must have been assigned the Security Administrator role.

Procedure

1 In the **Policy** tab of the Data Security panel, expand **Files to scan**.

2 Click **Edit**.

3 You can either monitor all files on the virtual machines in your inventory, or select the restrictions you want to apply.

Option	Description
Monitor all files on the guest virtual machines	vShield Data Security scans all files.
Monitor only the files that match the following conditions	Select the following options as appropriate. ■ **Size** indicates that vShield Data Security should only scan files less than the specified size. ■ **Last Modified Date** indicates that vShield Data Security should scan only files modified between the specified dates. ■ **Types:** Select **Only files with the following extensions** to enter the file types to scan. Select **All files, except those with extensions** to enter the file types to exclude from the scan.

For information on file formats that vShield Data Security can detect, see "Supported File Formats," on page 223.

4 Click **Save.**

5 If you are updating an existing policy, click **Publish Changes** to apply it.

Editing a Data Security Policy

After you have defined a data security policy, you can edit it by changing the regulations selected, areas participating in the scan, or the file filters. To apply the edited policy, you must publish it.

Prerequisites

Verify that you have been assigned the Security Administrator role.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select a datacenter.

NOTE Even though you are selecting a datacenter, the edited policy will be applied to the entire vSphere inventory.

3 Click the **vShield** tab and click **Data Security**.

4 Click the **Policy** tab and expand sections that you want to edit.

5 Make changes as appropriate.

6 Click **Save**.

7 If you are updating an existing policy, click **Publish Changes** to apply it.

NOTE If you publish a policy while a scan is running, the scan restarts. This rescan ensures that all virtual machines comply with the edited policy.

Running a Data Security Scan

Running a data security scan identifies data in your virtual environment that violates your policy.

Prerequisites

You must be a vShield Administrator to start, pause, or stop a data security scan.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Click the **vShield** tab and click **Data Security**.

3 Click **Start**.

NOTE If a virtual machine is powered off, it will not be scanned till it is powered on.

If a scan is in progress, the available options are **Pause** and **Stop**.

All virtual machines in your datacenter are scanned once during a scan. If the policy is edited and published while a scan is running, the scan restarts. This rescan ensures that all virtual machines comply with the edited policy. A rescan is triggered by publishing an edited policy, not by data updates on your virtual machines.

If a virtual machine is moved to an excluded cluster or resource pool while the data security scan is in progress, the files on that virtual machine are not scanned. In case a virtual machine is moved via vMotion to another host, the scan continues on the second host (files that were scanned while the virtual machine was on the previous host are not scanned again).

When the Data Security engine starts scanning a virtual machine, it records the scan start time. When the scan ends, it records the end of the scan. You can view the scan start and end time for a cluster, host, or virtual machine by selecting the **Tasks and Events** tab.

vShield Data Security throttles the number of virtual machines scanned on a host at a time to minimize impact on performance. VMware recommends that you pause the scan during normal business hours to avoid any performance overhead.

Viewing and Downloading Reports

When you start a security scan, vShield displays the start and end time of each scan, the number of virtual machines scanned, and the number of violations detected.

Prerequisites

Verify that you have been assigned the Security Administrator or Auditor role.

Procedure

1 In the vSphere Client, select **Inventory > Hosts and Clusters**.

2 Select the datacenter, cluster, resource pool, or virtual machine for which you want to view reports.

3 Click the **vShield** tab.

4 Click the **Data Security** tab.

5 Ensure that you are in the **Reports** tab.

Table 15-1. Information displayed in the Reports tab

Section	Information Displayed
Current Scan Status	Status of the current scan.
Scan Statistics	Pie chart displays the number of virtual machines which have been scanned, are being scanned, and have not started being scanned.
Violation Information	Top regulations that have been violated and the virtual machines on which the most violations have been reported.
Scan History	Start and end time of each scan, the number of virtual machines scanned, and the number of violations detected. You can click **Download Complete Report** in the **Action** column to download the complete report for any scan.

Creating Regular Expressions

A regular expression is a pattern that describes a certain sequence of text characters, otherwise known as strings. You use regular expressions to search for, or match, specific strings or classes of strings in a body of text.

Using a regular expression is like performing a wildcard search, but regular expressions are far more powerful. Regular expressions can be very simple, or very complex. An example of a simple regular expression is *cat.*

This finds the first instance of the letter sequence cat in any body of text that you apply it to. If you want to make sure it only finds the word *cat*, and not other strings like *cats* or *hepcat*, you could use this slightly more complex one: *\bcat\b*.

This expression includes special characters that make sure a match occurs only if there are word breaks on both sides of the *cat* sequence. As another example, to perform a near equivalent to the typical wildcard search string *c+t*, you could use this regular expression: *\bc\w+t\b*.

This means find a word boundary (\b) followed by a *c*, followed by one or more non-whitespace, non-punctuation characters (\w+), followed by a *t*, followed by a word boundary (\b). This expression finds *cot*, *cat*, *croat*, but not *crate.*

Expressions can get very complex. The following expression finds any valid email address.

\b[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b

For more information on creating regular expressions, see http://userguide.icu-project.org/strings/regexp.

Available Regulations

Below are descriptions of each of the regulations available within vShield Data Security.

Arizona SB-1338

Arizona SB-1338 is a state data privacy law which protects personally identifiable information. Arizona SB-1338 was signed into law April 26, 2006 and became effective December 31, 2006. The law applies to any person or entity that conducts business in Arizona and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data

- US Drivers License Number
- US Social Security Number

ABA Routing Numbers

A routing transit number (RTN) or ABA number is a nine digit bank code, used in the United States, which appears on items such as checks that identifies which financial institution it is drawn upon. This code is also used by the Automated Clearing House to process direct deposits and other automated transfers. This system is named after the American Bankers Association, which designed it in 1910.

There are approximately 24,000 active routing and transit numbers currently in use. Every financial institution has one of these; it is a 9-digit number printed in MICR font at the bottom of checks that specifically identifies which financial institution it is associated with, and it is governed by the Routing Number Administrative Board which is sponsored by the ABA.

The primary purposes of the routing number are:

- To identify the bank which is responsible to either pay or give credit or is entitled to receive payment or credit for a financial transaction.
- To provide a reference to a designated presentment point of the bank at which the transaction can be delivered or presented.

For more information, see "ABA Routing Number Content Blade," on page 204.

Australia Bank Account Numbers

An Australian bank account number, along with a BSB (Bank-State-Branch number) identifies the bank account of an individual or organization.

Australia Business and Company Numbers

Australia Business Numbers (ABN) and Australia Company Numbers (ACN) uniquely identify businesses within the country.

The ABN is a unique 11-digit identifying number that businesses use when dealing with other businesses. A company's ABN frequently includes the ACN as the last nine digits. The ABN indicates that a person, trust or company is registered with the Australian Business Register (ABR).

An Australian Company Number (usually shortened to ACN) is a unique 9-digit number issued by the Australian Securities and Investments Commission (ASIC) to every company registered under the Commonwealth Corporations Act 2001 as an identifier. The number is usually printed in three groups of three digits.

Companies are required to disclose their ACN on:

- the common seal (if any)
- every public document issued, signed or published by, or on behalf of, the company
- every eligible negotiable instrument issued, signed or published by, or on behalf of, the company
- all documents required to be lodged with ASIC

This regulation uses the content blades titled Australia Business Number or Australia Company Number. For more information, see.

Australia Medicare Card Numbers

All Australian citizens and permanent residents of Australia and their families are eligible for a Medicare Card, with the exception of residents on Norfolk Island. The card lists an individual as well as members of his or her family he or she chooses to add who are also permanent residents and meet the Medicare definition of a dependent (maximum of five names). It is necessary to provide a Medicare Number for a Medicare rebate or to gain access to the public hospital system to be treated at no cost as a public patient.

Medicare is administered by Medicare Australia (known as the Health Insurance Commission until late 2005) which also has the responsibility for supplying Medicare cards and numbers. Almost every eligible person has a card: in June 2002 there were 20.4 million Medicare card-holders, and the Australian population was less than 20 million at the time (card-holders includes overseas Australians who still have a card).

The Medicare card is used for health care purposes only and cannot be used to track in a database. It contains a name and number, and no visible photograph (with the exception of the Tasmanian "Smartcard" version which does have an electronic image of the cardholder on an embedded chip).

The primary purpose of the Medicare card is to prove Medicare eligibility when seeking Medicare-subsidized care from a medical practitioner or hospital. Legally, the card need not be produced and a Medicare number is sufficient. In practice, most Medicare providers will have policies requiring the card be presented to prevent fraud.

Australia Tax File Numbers

A Tax File Number (TFN) is a number that is issued to a person by the Commissioner of Taxation and is used to verify client identity and establish income level.

This policy uses the content blade titled Australia Tax File Number. Refer to the description of the content blades to understand what content will be detected.

California AB-1298

California AB-1298 is a state data privacy law which protects personally identifiable information. California AB-1298 in was signed into law October 14, 2007 and became effective January 1, 2008. The law applies to any person, business, or state agency that conducts business in California and owns or licenses unencrypted computerized data that includes personally identifiable information.

This law is an amendment to California SB-1386 to include medical information and health information in the definition of personal information.

The regulation looks for at least one match to personally identifiable information, as defined through the following content blades:

- Admittance and Discharge Dates
- Credit Card Numbers
- Credit Card Track Data
- Group Insurance Numbers
- Health Plan Beneficiary Numbers
- Healthcare Dictionaries
- Medical History
- Patient Identification Numbers
- US Drivers License Numbers

- US National Provider Identifiers
- US Social Security Numbers

California SB-1386

California SB-1386 is a state data privacy law which protects personally identifiable information. California SB-1386 was signed into law September 25, 2002 and became effective July 1, 2003. The law applies to any person, business, or state agency that conducts business in California and owns or licenses unencrypted computerized data that includes personally identifiable information.

This law has been amended to include medical information and health information; it is now referred to as California AB-1298, which is provided as an expanded regulation in the SDK. If California AB-1298 is enabled, you do not need to also use this regulation as the same information is detected as part of AB-1298.

The regulation looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Canada Social Insurance Numbers

A Social Insurance Number (SIN) is a number issued in Canada to administer various government programs. The SIN was created in 1964 to serve as a client account number in the administration of the Canada Pension Plan and Canada's varied employment insurance programs. In 1967, Revenue Canada (now the Canada Revenue Agency) started using the SIN for tax reporting purposes.

Canada Drivers License Numbers

In Canada, driver's licenses are issued by the government of the province in which the driver resides. Thus, specific regulations relating to driver's licenses vary province to province, though overall they are quite similar. All provinces have provisions allowing non-residents to use licenses issued by other provinces and International Driving Permits.

The regulation looks for at least a match to at least one of the following content blades:

- Alberta Drivers Licence
- British Columbia Drivers Licence
- Manitoba Drivers Licence
- New Brunswick Drivers Licence
- Newfoundland and Labrador Drivers Licence
- Nova Scotia Drivers Licence

  License pattern rules: 5 letters followed by 9 digits
- Ontario Drivers Licence
- Prince Edward Island Drivers Licence
- Quebec Drivers Licence
- Saskatchewan Drivers Licence

Colorado HB-1119

Colorado HB-1119 is a state data privacy law which protects personally identifiable information. Colorado HB-1119 was signed into law April 24, 2006 and became effective September 1, 2006. The law applies to any individual or a commercial entity that conducts business in Colorado and owns or licenses unencrypted computerized data that includes personally identifiable information.

The regulation looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Connecticut SB-650

Connecticut SB-650 is a state data privacy law which protects personally identifiable information. Connecticut SB-650 was signed into law June 8, 2005 and became effective January 1, 2006. The law applies to any person, business or agency that conducts business in Connecticut and owns or licenses unencrypted computerized data that includes personally identifiable information.

The regulation looks for at least one match to personally identifiable information, as defined through the following content blades:

- Admittance and Discharge Dates
- Birth and Death Certificates
- Credit Card Numbers
- Credit Card Track Data
- Group Insurance Numbers
- Health Plan Beneficiary Numbers
- Healthcare Dictionaries
- Medical History
- Patient Identification Numbers
- US Drivers License Numbers
- US National Provider Identifiers
- US Social Security Numbers

Credit Card Numbers

Custom Account Numbers

If you have organizational account numbers that need to be protected, then customize the content blade assigned to the Custom Account Numbers regulation with the number pattern via a regular expression.

EU Debit Card Numbers

The policy looks for debit card numbers as issued by the major debit card carriers in the European Union such as Maestro, Visa and Laser.

FERPA (Family Educational Rights and Privacy Act)

FERPA protects the privacy of student records at educational institutions receiving U.S. Department of Education funds. It requires the educational institution to have written permission from a parent or student in order to release information from a student's educational record.

Under certain circumstances the release of information such as name, address, telephone number, honors and awards, and dates of attendance may be released or published without permission. Information that can connect an individual with grades or disciplinary actions requires permission.

The policy must match both of the following content blades for a document to trigger as a violation:

- Student Identification Numbers
- Student Records

Florida HB-481

Florida HB-481 is a state data privacy law which protects personally identifiable information. Florida HB-481 was signed into law June 14, 2005 and became effective July 1, 2005. The law applies to any person, firm, association, joint venture, partnership, syndicate, corporation, and all other groups or combinations that conduct business in Florida and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

France IBAN Numbers

A France International Bank Account Number (IBAN) is an international standard for identifying France bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade France IBAN Number.

France National Identification Numbers Policy

The policy identifies documents and transmissions that contain national identification numbers, also called INSEE numbers and Social Security numbers, issued to individuals at birth by the Institut National de la Statistique et des Etudes Economiques (INSEE) in France.

The policy looks for a match to the content blade France National Identification Number.

Georgia SB-230 Policy

Georgia SB-230 is a state data privacy law which protects personally identifiable information. Georgia SB-230 was signed into law May 5, 2005 and became effective May 5, 2005. The law applies to any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personally identifiable information to nonaffiliated third parties, or any state or local agency or subdivision thereof that maintains data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Germany BIC Numbers Policy

A Bank Identifier Code (BIC) uniquely identifies a particular bank and is used in France and worldwide for the exchange of money and messages between banks. The policy identifies documents and transmissions that contain BIC codes, also known as SWIFT codes, issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade Germany BIC Number.

Germany Driving License Numbers Policy

A Germany Drivers License Number is an identification number on a German Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Germany Driving License Number.

Germany IBAN Numbers Policy

International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade Germany IBAN Number.

Germany National Identification Numbers Policy

The policy identifies documents and transmissions that contain personal identification numbers, or Personalausweis, issued to individuals in Germany.

The policy looks for a match to the content blade Germany National Identification Number.

Germany VAT Numbers Policy

based business or legal entity for the purposes of levying Value Added Tax (or goods and services tax).

The policy looks for a match to the content blade Germany VAT Number.

Hawaii SB-2290 Policy

Hawaii SB-2290 is a state data privacy law which protects personally identifiable information.

Hawaii SB-2290 was signed into law May 25, 2006 and became effective January 1, 2007. The law applies to any sole proprietorship, partnership, corporation, association, or other group, however organized, and whether or not organized to operate at a profit, including financial institutions organized, chartered, or holding a license or authorization certificate under the laws of Hawaii, any other state, the US, or any other country, or the parent or the subsidiary of any such financial institution, and any entity whose business is records destruction, or any government agency that collects personally identifiable information for specific government purposes

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

HIPAA (Healthcare Insurance Portability and Accountability Act) Policy

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the Congress of the United States of America. HIPAA includes a Privacy Rule regulating the use and disclosure of protected health information (PHI), a Security Rule defining security safeguards required for electronic protected health information (ePHI), and an Enforcement Rule that defines procedures for violation investigations and penalties for confirmed violations.

PHI is defined as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records. Individually identifiable means the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

This policy is designed to detect electronic PHI, which contains a personal health number in addition to health-related terminology. Some false negatives may occur since combinations of personally identifiable information, such as name and address, would not be considered as ePHI with this policy. Internal research indicates that the majority of health communication will contain a personal health number in addition to health-related terminology.

Idaho SB-1374 Policy

Idaho SB-1374 is a state data privacy law which protects personally identifiable information. Idaho SB-1374 was signed into law March 30, 2006 and became effective July 1, 2006. The law applies to any agency, individual, or commercial entity that conducts business in Idaho and owns or licenses unencrypted computerized data that includes personally identifiable information about a resident of Idaho.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Illinois SB-1633

Illinois SB-1633 is a state data privacy law which protects personally identifiable information. Illinois SB-1633 was signed into law June 16, 2005 and became effective June 27, 2006.

The law applies to any data collector, which includes, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personally identifiable information that owns or licenses personally identifiable information concerning an Illinois resident.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Indiana HB-1101 Policy

Indiana HB-1101 is a state data privacy law which protects personally identifiable information. Indiana HB-1101 was signed into law April 26, 2005 and became effective July 1, 2006. The law applies to any individual, corporation, business trust, estate, trust partnership, association, nonprofit corporation or organization, cooperative, or any other legal entity that owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Italy Driving License Numbers Policy

A Italy Drivers License Number is an identification number on a Italian Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Italy Driving License Number.

Italy IBAN Numbers Policy.

A International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

The policy looks for a match to the content blade Italy IBAN Number.

Italy National Identification Numbers Policy

The policy identifies documents and transmissions that contain personal identification numbers, or Codice Fiscale, issued to individuals in Italy.

The policy looks for a match to the content blade Italy National Identification Number.

Kansas SB-196 Policy

Kansas SB-196 is a state data privacy law which protects personally identifiable information. Kansas SB-196 was signed into law April 19, 2006 and became effective January 1, 2007. The law applies to any individual, partnership, corporation, trust, estate, cooperative, association, government, or government subdivision or agency or other entity that conducts business in Kansas and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Louisiana SB-205 Policy

Louisiana SB-205 is a state data privacy law which protects personally identifiable information. Louisiana SB-205 was signed into law July 12, 2005 and became effective January 1, 2006. The law applies to any individual, corporation, partnership, sole proprietorship, joint stock company, joint venture, or any other legal entity that conducts business in Louisiana and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Maine LD-1671 Policy

Maine LD-1671 is a state data privacy law which protects personally identifiable information. Maine LD-1671 was signed into law June 10, 2005 and became effective January 31, 2006.

The law applies to any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity, including agencies of state government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private collages and universities, or any information in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personally identifiable information to nonaffiliated third parties that maintains computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Massachusetts CMR-201

Massachusetts CMR-201 is a state data privacy regulation which protects personally identifiable information. Massachusetts CMR-201 was issued on September 19, 2008 and became effective May 1, 2009. The regulation applies to all businesses and other legal entities that own, license, collect, store or maintain personal information about a resident of the Commonwealth of Massachusetts.

The policy looks for at least one match to personally identifiable information, which may include:

- ABA Routing Numbers
- Credit Card Number
- Credit Card Track Data
- US Bank Account Numbers
- US Drivers License Number
- US Social Security Number

Minnesota HF-2121

Minnesota HF-2121 is a state data privacy law which protects personally identifiable information. Minnesota HF-2121 was signed into law June 2, 2005 and became effective January 1, 2006. The law applies to any person or business that conducts business in Minnesota and owns or licenses data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Montana HB-732

Montana HB-732 is a state data privacy law which protects personally identifiable information. Montana HB-732 was signed into law April 28, 2005 and became effective March 1, 2006. The law applies to any person or business that conducts business in Montana and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Netherlands Driving Licence Numbers

A Netherlands Driving License number is an identification number on a Netherlands Drivers License and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade Netherlands Driving License Number.

Nevada SB-347

Nevada SB-347 is a state data privacy law which protects personally identifiable information. Nevada SB-347 was signed into law June 17, 2005 and became effective October 1, 2005. The law applies to any government agency, institution of higher education, corporation, financial institution or retail operator, or any other type of business entity or association that owns or

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Hampshire HB-1660

New Hampshire HB-1660 is a state data privacy law which protects personally identifiable information. New Hampshire HB-1660 was signed into law June 2, 2006 and became effective January 1, 2007. The law applies to any individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company, or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state doing business in New Hampshire that owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Jersey A-4001

New Jersey A-4001 is a state data privacy law which protects personally identifiable information.

New Jersey A-4001 was signed into law September 22, 2005 and became effective January 1, 2006. The law applies to New Jersey, and any country, municipality, district, public authority, public agency, and any other political subdivision or public body in New Jersey, any sole proprietorship, partnership, corporation, association, or other entity, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of New Jersey, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution, that conducts business in New Jersey that compiles or maintains computerized records that include personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New York AB-4254

New York AB-4254 is a state data privacy law which protects personally identifiable information. New York AB-4254 was signed into law August 10, 2005 and became effective December 8, 2005. The law applies to any person or business which conducts business in New York and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

New Zealand Inland Revenue Department Numbers

The policy identifies documents and transmissions that contain New Zealand Inland Revenue Department (IRD) numbers issued by the Inland Revenue Department to every taxpayer and organization. The number must be provided by an individual to the Inland Revenue, employers, banks or other financial institutions, KiwiSaver scheme providers, StudyLink and tax agents.

The policy looks for a match to the content blade New Zealand Inland Revenue Department Number.

New Zealand Ministry of Health Numbers

The policy identifies documents and transmissions that contain New Zealand Health Practitioner Index (HPI) or National Health Index (NHI) numbers.

The New Zealand Ministry of Health, or Manatū Hauora in Māori, is the New Zealand government's principal agent and advisor on health and disability. The agency uses the NHI numbering system for registering patients and the HPI system for registering medical practitioners to ensure that records are accurate while protecting the privacy of individuals. This policy detects 6-digit alphanumeric New Zealand Health Practitioner Index Common Person numbers (HPI-CPN), which uniquely identify a health practitioner or worker. This policy also detects 7-digit NHI numbers used to uniquely identify a patient within the New Zealand health system.

The policy looks for a match to either of the content blades:

- New Zealand Health Practitioner Index Number
- New Zealand National Health Index Number

Ohio HB-104

Ohio HB-104 is a state data privacy law which protects personally identifiable information. Ohio HB-104 was signed into law November 17, 2005 and became effective December 29, 2006. The law applies to any individual, corporation, business trust, estate, trust, partnership, or association that conducts business in Ohio and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Oklahoma HB-2357

Oklahoma HB-2357 is a state data privacy law which protects personally identifiable information. Oklahoma HB-2357 was signed into law June 8, 2006 and became effective November 1, 2008. The law applies to any corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit that conducts business in Oklahoma HB-2357 and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Patient Identification Numbers

The personally identifiable information (PII) commonly held by hospitals and healthcare-related organizations and businesses in the United States of America. This policy should be customized to define the patient identification number format.

The policy looks for at least one match to personally identifiable information, which may include:

- Patient Identification Numbers
- US National Provider Identifier
- US Social Security Number

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The policy looks for at least one match to either of the content blades:

- Credit Card Number
- Credit Card Track Data

Texas SB-122

Texas SB-122 is a state data privacy law which protects personally identifiable information. Texas SB-122 was signed into law June 17, 2005 and became effective September 1, 2005. The law applies to any person that conducts business in Texas and owns or licenses unencrypted computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data

- US Drivers License Number
- US Social Security Number

UK BIC Numbers

A Bank Identifier Code (BIC) uniquely identifies a particular bank and is used in the UK and worldwide for the exchange of money and messages between banks. The policy identifies documents and transmissions that contain BIC codes, also known as SWIFT codes, issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade UK BIC Number.

UK Driving Licence Numbers

A UK driving license number is an identification number on a UK driving license and identifies the owner of said number for the purposes of driving and driving offences.

The policy looks for a match to the content blade UK Driving License Number.

UK IBAN Numbers

International Bank Account Number (IBAN) is an international standard for identifying the UK bank accounts across national borders and was originally adopted by the European Committee for Banking Standards. The official IBAN registrar under ISO 13616:2003 is issued by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The policy looks for a match to the content blade UK IBAN Number.

UK National Health Service Numbers

A UK National Health Service number is an identification number provided by the UK National Health Service and identifies the owner of said number for the purposes of medical records.

The policy looks for a match to the content blade UK National Health Service Number.

UK National Insurance Numbers (NINO)

UK National Insurance is a system of payments made out of earnings by employees, employers and the self-employed to the Government that entitle you to a state pension and other benefits.

UK National Insurance Numbers (NINO) are the identification numbers assigned to each person born in the UK, or to anyone resident in the UK who is a legal employee, student, recipient of social welfare benefits, pension etc.

The policy looks for a match at least one of the content blades UK NINO Formal or UK NINO Informal.

UK Passport Numbers

The policy identifies documents and transmissions that contain passport numbers issued in the UK.

The policy looks for a match to the content blade UK Passport Number.

US Drivers License Numbers

Driver's licenses issued in the United States have a number or alphanumeric code issued by the Department of Motor Vehicles (or equivalent), usually show a photograph of the bearer, as well as a copy of his or her signature, the address of his or her primary residence, the type or class of license, restrictions and/or endorsements (if any), the physical characteristics of the bearer (such as height, weight, hair color, eye color, and sometimes even skin color), and birth date. No two driver's license numbers issued by a state are alike. Social Security numbers are becoming less common on driver's licenses, due to identity theft concerns.

The policy looks for a match to the content blade US Drivers Licenses.

US Social Security Numbers

The U.S. Social Security number is issued to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2). The number is issued to an individual by the Social Security Administration, an independent agency of the United States government. Its primary purpose is to track individuals for taxation purposes.

Utah SB-69

Utah SB-69 is a state data privacy law which protects personally identifiable information. Utah SB-69 was signed into law March 20, 2006 and became effective January 1, 2007. The law applies to any who owns or license computerized data that includes personally identifiable information concerning a Utah resident.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Vermont SB-284

Vermont SB-284 is a state data privacy law which protects personally identifiable information. Vermont SB-284 was signed into law May 18, 2006 and became effective January 1, 2007. The law applies to any data collector that owns or licenses unencrypted computerized data that includes personally identifiable information concerning an individual residing in Vermont.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number
- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Washington SB-6043

Washington SB-6043 is a state data privacy law which protects personally identifiable information. Washington SB-6043 was signed into law May 10, 2005 and became effective July 24, 2005. The law applies to any state or local agency or any person or business which conducts business in Washington and owns or licenses computerized data that includes personally identifiable information.

The policy looks for at least one match to personally identifiable information, which may include:

- Credit Card Number

- Credit Card Track Data
- US Drivers License Number
- US Social Security Number

Available Content Blades

This sections lists the available content blades for vShield regulations.

ABA Routing Number Content Blade

The content blade looks for matches to 3 pieces of information in close proximity of each other.

The content blade looks for:

- ABA routing number
- Banking words and phrases (e.g. aba, routing number, checking, savings)
- Personally identifiable information (e.g. name, address, phone number)

Words and phrases related to banking are implemented in order to increase precision. A routing number is 9-digits and may pass for many different data types, for example, a valid US Social Security number, Canadian Social Insurance number or international telephone number.

Since routing numbers themselves are not sensitive, personally identifiable information is necessary for a violation to occur.

Admittance and Discharge Dates Content Blade

The content blade looks for matches to the U. S. Date Format entity and words and phrases such as admit date, admittance date, date of discharge, discharge date in close proximity to each other.

Alabama Drivers License Content Blade

The content blade looks for matches to the Alabama driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AL or Alabama.

Driver's license pattern

7 Numeric or 8 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alaska driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern

7 Numeric

Alaska Drivers License Content Blade

The content blade looks for matches to the Alaska driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern:

7 Numeric

Alberta Drivers Licence Content Blade

The content blade looks for matches to the Alaska driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AK or Alaska.

Driver's license pattern

7 Numeric

American Express Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one American Express credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Arizona Drivers License Content Blade

The content blade looks for matches to the Arizona driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AZ or Arizona.

The Driver's license pattern can be 1 Alphabetic, 8 Numeric; or 9 Numeric (SSN); or 9 Numeric (Unformatted SSN).

Arkansas Drivers License Content Blade

The content blade looks for matches to the Arizona driver's license pattern and words and phrases such as driver's license and license number and, optionally, terms such as AR or Arkansas.

Driver's license pattern can be 9, 8 Numeric.

Australia Bank Account Number Content Blade

The Australian bank account number itself is not sensitive, but identifies a bank account, without identifying the bank branch. Therefore, both the account number and branch information must exist for the document to be considered sensitive.

The content blade looks for matches to both:

- An Australian bank account number
- Words and phrases related to bank state branch or BSB.

It also uses a regular expression rule to differentiate between telephone numbers of the same length.

An Australian bank account number is 6 to 10-digits without any embedded meaning. It has no check digit routine.

Australia Business Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Business Number
- ABN words and phrases (e.g. ABN, Australia business number)

Australia Company Number Content Blade

The content blade looks for matches to both pieces of information in close proximity to each other.

- Australia Company Number
- ACN words and phrases (e.g. ACN, Australia Company Number)

Australia Medicare Card Number Content Blade

The content blade will match if one of the following combinations of information appears in a document.

- More than one Australia Medicare Card Number
- One Medicare card number plus Medicare or patient identification terms (e.g. patient identifier, patient number)
- One Medicare card number plus two of either a name, expiration date or expiration terms

Australia Tax File Number Content Blade

The content blade looks for matches to both pieces of information in high proximity to each other.

- Australia Tax File Number (refer to entity description)
- Tax file number words and phrases (e.g. TFN, tax file number)

California Drivers License Number Content Blade

The content blade looks for matches to the California driver's license pattern and words and phrases such as driver's license and license number and terms such as CA or California.

The Driver's license pattern is 1 Alphabetic, 7 Numeric.

Canada Drivers License Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for driver's licenses in individual providences and territories.

Canada Social Insurance Number Content Blade

The content blade is only a container file for child content blades. The content blades assigned to it separately look for formatted and unformatted versions of the Canadian Social Insurance numbers plus personal information so different rules may be assigned to them. The formatted version of the Social Insurance number is a more specific pattern, so the rules are less strict for retuning a match. However, the unformatted version is very general and matches to many common numbers.

Colorado Drivers License Number Content Blade

The content blade looks for matches to the Colorado driver's license pattern and words and phrases such as driver's license and license number and terms such as CO or Colorado.

The driver's license pattern is 9 Numeric.

Connecticut Drivers License Number Content Blade

The content blade looks for matches to the Connecticut driver's license pattern and words and phrases such as driver's license and license number and terms such as CT or Connecticut.

Driver's license pattern: 9 Numeric, 1st two positions are month of birth in odd or even year. 01-12 Jan-Dec odd years, 13-24 Jan-Dec even years, 99 unknown.

Credit Card Number Content Blade

The content blade looks for a combination of the following pieces of information.

- More than one credit card number
- A single credit card number plus words and phrases such as ccn, credit card, expiration date
- A single credit card number plus an expiration date

Credit Card Track Data Content Blade

Track data is the information encoded and stored on two tracks located within the magnetic stripe on the back of a credit card (debit card, gift card, etc). There are three tracks on the magstripe (magnetic strip on the back of a credit card).

Each track is .110-inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 six-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 four-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 four-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (that includes an encrypted PIN, country code, currency units, amount authorized), but its usage is not standardized among banks.

This content blade requires a match to the Credit Card Track Data entity.

Custom Account Number Content Blade

The Custom Accounts content blade is an editable blade and should contain a regular expression for an organization's custom account patterns.

Delaware Drivers License Number Content Blade

The content blade looks for matches to the Delaware driver's license pattern and words and phrases such as driver's license and license number and terms such as DE or Delaware.

EU Debit Card Number Content Blade

The content blade looks for patterns of the major European Union debit card numbers.

The content blade will match with a combination of the following pieces of information in close proximity, if either:

- More than one match to a EU debit card number
- A single match to a EU debit card number plus two of either a word or phrase for credit card (e.g. card number or cc#), credit card security, expiration date or name
- A single match to a EU debit card number with an expiration date

Florida Drivers License Number Content Blade

The content blade looks for matches to the Florida driver's license pattern and words and phrases such as driver's license and license number and terms such as FL or Florida.

Driver's license pattern: 1 Alphabetic, 12 Numeric.

France Driving License Number Content Blade

The content blade requires the following to match for a French driving license in a close proximity.

- French driving license pattern
- Either words or phrases for a driving license (e.g. driving license, permis de conduire) or E.U. date format

France BIC Number Content Blade

The content blade scans for French BIC numbers by requiring matches for both the following rules.

- European BIC number format
- French format of the BIC number

France IBAN Number Content Blade

The content blade requires the following to match for a French IBAN number in a close proximity.

- European IBAN number format
- French IBAN number pattern

France National Identification Number Content Blade

The content blade requires the following to match for a French National Identification number in a close proximity.

- More than one match to the French National Identification pattern
- One match to the French National Identification pattern plus either words or phrases for a social security number (e

France VAT Number Content Blade

The content blade requires a match for a French value added tax (VAT) number pattern in a close proximity to the abbreviation FR.

Georgia Drivers License Number Content Blade

The content blade looks for matches to the Georgia driver's license pattern and words and phrases such as driver's license and license number and terms such as GA or Georgia.

Driver's license pattern: 7-9 Numeric; or Formatted SSN.

Germany BIC Number Content Blade

The content blade scans for German BIC numbers by requiring matches for both the following rules.

- European BIC number format
- German format of the BIC number

Germany Driving License Number Content Blade

The content blade requires the following to match for a German driving license in a close proximity.

- German driving license pattern\
- Words or phrases related to a driving license (e.g. driving license, ausstellungsdatum)

Germany IBAN Number Content Blade

The content blade requires the following to match for a German IBAN number in a close proximity.

- European IBAN number format
- German IBAN number pattern

THe German IBAN rule: "DE" country code followed by 22 digits.

Germany National Identification Numbers Content Blade

The content blade requires the following to match for a German National Identification number in a close proximity.

- Either a German National Identification number or a machine-readable version of the number
- Words or phrases for a German National Identification number (e.g. personalausweis, personalausweisnummer)

Germany Passport Number Content Blade

The content blade requires the following to match for a German passport number in a close proximity.

- Either a German passport number or a machine-readable version of the number
- Words or phrases for a German passport number or issuance date (e.g. reisepass, ausstellungsdatum)

Germany VAT Number Content Blade

The content blade requires a match for a German value added tax (VAT) number pattern (refer to entity description) in a close proximity to the abbreviation DE.

Group Insurance Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression to match the number pattern for an organization's Group Insurance Number. The content blade looks for matches to words and phrases such as group insurance or a name, U.S. address or U.S. date in combination with the custom regular expression.

Hawaii Drivers License Number Content Blade

The content blade looks for matches to the Hawaii driver’s license pattern and words and phrases such as driver’s license and license number and terms such as HI or Hawaii.

Driver's license pattern: H Alphabetic, 8 Numeric; or SSN.

Italy National Identification Numbers Content Blade

The content blade requires the following to match for an Italy National Identification number in a close proximity.

1 Italy National Identification number pattern

2 Words or phrases for an Italy National Identification number (e.g. codice fiscale, national identification)

National Identification Rule: 16 character alphanumeric code. where:

- *SSS* are the first three consonants in the family name (the first vowel and then an X are used if there are not enough consonants)
- *NNN* is the first name, of which the first, third and fourth consonants are used—exceptions are handled as in family names
- *YY* are the last digits of the birth year
- *M* is the letter for the month of birth—letters are used in alphabetical order, but only the letters A to E, H, L, M, P, R to T are used (thus, January is A and October is R)
- *DD* is the day of the month of birth—in order to differentiate between genders, 40 is added to the day of birth for women (thus a woman born on May 3 has ...E43...)
- *ZZZZ* is an area code specific to the municipality where the person was born—country-wide codes are used for foreign countries, a letter followed by three digits
- *X* is a parity character as calculated by adding together characters in the even and odd positions, and dividing them by 26. Numerical values are used for letters in even positions according to their alphabetical order. Characters in odd positions have different values. A letter is then used which corresponds to the value of the remainder of the division in the alphabet.

Pattern:

- *LLLLLLDDLDDLDDDL*
- *LLL LLL DDLDD LDDDL*

Health Plan Beneficiary Numbers

This is a content blade that requires customization. To use this content blade, add a regular expression to identify recipients of health plan benefits and payments. The content blade looks for matches to words and phrases such as beneficiary or a name, U.S. address or U.S. date in combination with the custom regular expression.

Idaho Drivers License Number Content Blade

The content blade looks for matches to the Idaho driver's license pattern and words and phrases such as driver's license and license number and terms such as ID or Idaho.

Driver's license pattern: 2 Alphabetic, 6 Numeric, 1 Alphabetic.

Illinois Drivers License Number Content Blade

The content blade looks for matches to the Illinois driver's license pattern and words and phrases such as driver's license and license number and terms such as IL or Illinois.

Driver's license pattern: 1 Alphabetic, 11 Numeric.

Indiana Drivers License Number Content Blade

The content blade looks for matches to the Indiana driver's license pattern and words and phrases such as driver's license and license number and terms such as IN or Indiana.

Driver's license pattern: 10 Numeric.

Iowa Drivers License Number Content Blade

The content blade looks for matches to the Iowa driver's license pattern and words and phrases such as driver's license and license number and terms such as IA or Iowa.

Driver's license pattern can be 3 numeric, 2 alphabetic, 3 numeric; or Social Security Number.

Index of Procedures Content Blade

The content blade looks for words and phrases related to medical procedures based on the International Classification of Diseases (ICD).

The content blade will match with a combination of the following pieces of information, either:

- More than one match to the Index of Procedures dictionary
- A single match to the Index of Procedures dictionary plus two of either a name, U.S. Address or U.S. Date
- A single match to the Index of Procedures dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Italy Driving License Number Content Blade

The content blade requires the following to match for an Italy driving license in a close proximity.

- Italy driving license pattern
- Words or phrases for a driving license (e.g. driving license, patente di guida)

Driver's License Rule: 10 alphanumeric characters -- 2 letters, 7 numbers and a final letter. The first letter may only be characters A-V.

Driver's License Pattern:

- *LLDDDDDDDL*
- *LL DDDDDDD* L
- *LL-DDDDDDD-L*
- *LL - DDDDDDD - L*

Italy IBAN Number Content Blade

The content blade requires the following to match for a Italy IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Italy IBAN number pattern

IBAN Rule: IT country code followed by 25 alphanumeric characters.

Pattern:

- IT*DDLDDDDDDDDDDAAAAAAAAAAAA*
- IT *DDL DDDDD DDDDD AAAAAAAAAAAA*
- IT *DD LDDDDD DDDDD AAAAAAAAAAAA*
- IT *DD L DDDDD DDDDD AAAAAAAAAAAA*
- IT *DD LDDDDDDDDDDAAAAAAAAAAAA*
- IT *DD L DDDDDDDDDDAAAAAAAAAAAA*

- IT*DD LDDD DDDD DDDA AAAA AAAA AAA*
- IT *DDL DDDDD DDDDD AAAAAA AAAAAA*
- IT *DDL DDD DDD DDD DAAA AAA AAAAAA*
- IT *DDL DDDDDDDDDD AAAAAA AAAAAA*

Spaces may be substituted with dashes, forward slashes or colons.

ITIN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Taxpayer Identification Number (ITIN). The content blade will match if an unformatted ITIN is found within close proximity of a word or phrase for an ITIN number (e.g. tax identification, ITIN).

ITIN Rule: 9-digit number that always begins with the number 9 and has a range of 70-88 in the fourth and fifth digit.

Pattern: *DDDDDDDDD*

Kansas Drivers License Number Content Blade

The content blade looks for matches to the Kansas driver's license pattern and words and phrases such as driver's license and license number and terms such as KS or Kansas.

Driver's license pattern: 1 Alphabetic (K), 8 Numeric; or Social Security Number.

Kentucky Drivers License Number Content Blade

The content blade looks for matches to the Kentucky driver's license pattern and words and phrases such as driver's license and license number and terms such as KY or Kentucky.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or Social Security Number.

Louisiana Drivers License Number Content Blade

The content blade looks for matches to the Louisiana driver's license pattern and words and phrases such as driver's license and license number and terms such as LA or Louisiana.

Driver's license pattern: 2 Zeros, 7 Numeric.

Maine Drivers License Number Content Blade

The content blade looks for matches to the Maine driver's license pattern and words and phrases such as driver's license and license number and terms such as ME or Maine.

Driver's license pattern: 7 Numeric, optional alphabetic X.

Manitoba Drivers Licence Content Blade

The content blade looks for matches to the Manitoba driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as MB or Manitoba in a close proximity.

License pattern rules: 12 alphanumeric characters that may be hyphen-separated, where:

- 1st character is a letter
- 2nd - 5th characters are a letter or asterisk
- 6th character is a letter
- 7th - 10th characters are digits

- 11th character is a letter
- 12th character is a letter or digit

or

- 1st character is a letter
- 2nd - 4th characters are a letter or asterisk
- 5th - 6th characters are digits
- 7th - 12th characters are a letter or digit

Driver's license pattern:

- *LLLLLLDDDDLA*
- *LLLLLDDAAAAAA*

Maryland Drivers License Number Content Blade

The content blade looks for matches to the Maryland driver's license pattern and words and phrases such as driver's license and license number and terms such as MD or Maryland.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Massachusetts Drivers License Number Content Blade

The content blade looks for matches to the Massachusetts driver's license pattern and words and phrases such as driver's license and license number and terms such as MA or Massachusetts.

Driver's license pattern: 1 Alphabetic (S), 8 Numeric; or Social Security Number

Michigan Drivers License Number Content Blade

The content blade looks for matches to the Michigan driver's license pattern and words and phrases such as driver's license and license number and terms such as MI or Michigan.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Minnesota Drivers License Number Content Blade

The content blade looks for matches to the Minnesota driver's license pattern and words and phrases such as driver's license and license number and terms such as MN or Minnesota.

Driver's license pattern: 1 Alphabetic, 12 Numeric

Mississippi Drivers License Number Content Blade

The content blade looks for matches to the Mississippi driver's license pattern and words and phrases such as driver's license and license number and terms such as MS or Mississippi.

Driver's license pattern: 9 Numeric; or Formatted Social Security Number

Missouri Drivers License Number Content Blade

The content blade looks for matches to the Missouri driver's license pattern and words and phrases such as driver's license and license number and terms such as MO or Missouri

Driver's license pattern: 1 Alphabetic, 6-9 Numeric; or 9 Numeric; or Formatted Social Security Number

Montana Drivers License Number Content Blade

The content blade looks for matches to the Montana driver's license pattern and words and phrases such as driver's license and license number and terms such as MT or Montana.

Driver's license pattern: 9 Numeric (SSN); or 1 Alphabetic, 1 Numeric, 1 Alphanumeric, 2 Numeric, 3 Alphabetic and 1 Numeric; or 13 Numeric

NDC Formulas Dictionary Content Blade

The content blade looks for words and phrases related to formulas based on the National Drug Codes (NDC).

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the NDC Formulas dictionary

2 A single match to the NDC Formulas dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the NDC Formulas dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Nebraska Drivers License Number Content Blade

The content blade looks for matches to the Nebraska driver's license pattern and words and phrases such as driver's license and license number and terms such as NE or Nebraska.

Driver's license pattern: 1 Alphabetic , 8 Numeric

Netherlands Driving Licence Number Content Blade

The content blade requires the following to match for a Netherlands driving license in a close proximity.

1 Netherlands driving license pattern (refer to entity description)

2 Words or phrases for a driving license (e.g. driving license, rijbewijs)

Netherlands IBAN Number Content Blade

The content blade requires the following to match for a Netherlands IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN)

2 Netherlands IBAN number pattern

IBAN Rule: NL country code followed by 16 alphanumeric characters.

Pattern:

- NL*DDLLLLDDDDDDDDDD*
- NL DDLLLLDDDDDDDDDD
- NL *DD LLLL DDDDDDDDDD*
- NL *DD LLLL DDDD DDDD DD*
- NL*DD LLLL DDDD DDDD DD*
- NL*DDLLLL DDDD DDDDDD*
- NL*DD LLLL DDDDDDDDDD*
- NL DD LLLL D DD DD DD DDD

- NL *DD LLLL DD DD DD DDDD*
- NL *DD LLLL DDD DDDDDDD*
- NL *DD LLLL DDDD DD DD DD*

Spaces may be substituted with dashes

Netherlands National Identification Numbers Content Blade

The content blade requires the following to match for a Netherlands National Identification number in a close proximity.

1 Netherlands National Identification number (refer to entity description)

2 Words or phrases for a Netherlands National Identification number (e.g. sofinummer, burgerservicenummer)

Netherlands Passport Number Content Blade

The content blade requires the following to match for a Netherlands passport number in a close proximity.

1 Netherlands passport number (refer to entity description)

2 Words or phrases for a Netherlands passport number (e.g. paspoort , Noodpaspoort)

Nevada Drivers License Number Content Blade

The content blade looks for matches to the Nevada driver's license pattern and words and phrases such as driver's license and license number and terms such as NV or Nevada.

Driver's license pattern: 9 Numeric (SSN); or 12 Numeric (last 2 are year of birth), or 10 numeric

New Brunswick Drivers Licence Content Blade

The content blade looks for matches to the New Brunswick driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NB or New Brunswick in a close proximity.

License pattern rules: 5 - 7 digits

Driver's license pattern:

- *DDDDD*
- *DDDDDD*
- *DDDDDDD*

New Hampshire Drivers License Number Content Blade

The content blade looks for matches to the New Hampshire driver's license pattern and words and phrases such as driver's license and license number and terms such as NH or New Hampshire.

Driver's license pattern: 2 Numeric, 3 Alphabetic, 5 Numeric

New Jersey Drivers License Number Content Blade

The content blade looks for matches to the New Jersey driver's license pattern and words and phrases such as driver's license and license number and terms such as NJ or New Jersey.

Driver's license pattern: 1 Alphabetic, 14 Numeric

New Mexico Drivers License Number Content Blade

The content blade looks for matches to the New Mexico driver's license pattern and words and phrases such as driver's license and license number and terms such as NM or New Mexico.

Driver's license pattern: 9 Numeric

New York Drivers License Number Content Blade

The content blade looks for matches to the New York driver's license pattern and words and phrases such as driver's license and license number and terms such as NY or New York.

Driver's license pattern: 9 Numeric

New Zealand Health Practitioner Index Number Content Blade

The content blade looks for matches to the New Zealand Health Practitioner Index entity and corroborative terms such as hpi-cpn or health practitioner index.

New Zealand Inland Revenue Department Number

The content blade looks for matches to the New Zealand Inland Revenue Department Number entity and words and phrases such as IRD Number or Inland Revenue Department Number.

New Zealand National Health Index Number Content Blade

The content blade looks for matches to the New Zealand National Health Index entity and corroborative terms such as nhi or National Health index.

Newfoundland and Labrador Drivers Licence Content Blade

The content blade looks for matches to the Newfoundland and Labrador driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NL or Labrador in a close proximity.

License pattern rules: 1 letter followed by 9 digits

Driver's license pattern: *LDDDDDDDDD*

North Carolina Drivers License Number Content Blade

The content blade looks for matches to the North Carolina driver's license pattern and words and phrases such as driver's license and license number and terms such as NC or North Carolina.

Driver's license pattern: 6 - 8 Numeric

North Dakota Drivers License Number Content Blade

The content blade looks for matches to the North Dakota driver's license pattern and words and phrases such as driver's license and license number and terms such as ND or North Dakota.

Driver's license pattern: 9 Numeric; or 3 Alphabetic, 6 Numeric

Nova Scotia Drivers Licence Content Blade

The content blade looks for matches to the Nova Scotia driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as NS or Nova Scotia in a close proximity.

License pattern rules: 5 letters followed by 9 digits

Driver's license pattern: *LLLLDDDDDDDDD*

Ohio Drivers License Number Content Blade

The content blade looks for matches to the Ohio driver's license pattern and words and phrases such as driver's license and license number and terms such as OH or Ohio.

Driver's license pattern: 2 Alphabetic, 6 Numeric

Oklahoma License Number Content Blade

The content blade looks for matches to the Oklahoma driver's license pattern and words and phrases such as driver's license and license number and terms such as OK or Oklahoma.

Driver's license pattern: 1 Alphabetic, 8 Numeric; or 9 Numeric; or Social Security Number, Formatted

Ontario Drivers Licence Content Blade

The content blade looks for matches to the Ontario driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as ON or Ontario in a close proximity.

License pattern rules: 1 letter followed by 14 digits

Driver's license pattern: *LDDDDDDDDDDDDD*

Oregon License Number Content Blade

The content blade looks for matches to the Oregon driver's license pattern and words and phrases such as driver's license and license number and terms such as OR or Oregon.

Driver's license pattern: 6 -7 Numeric

Patient Identification Numbers Content Blade

This is a content blade that requires customization. To use this content blade, add a regular expression for a company-specific Patient Identification Number pattern. The content blade looks for matches to words and phrases such as patient id or a name, U.S. address or U.S. date in combination with the custom regular expression.

Pennsylvania License Number Content Blade

The content blade looks for matches to the Pennsylvania driver's license pattern and words and phrases such as driver's license and license number and terms such as PA or Pennsylvania.

Driver's license pattern: 8 Numeric

Prince Edward Island Drivers Licence Content Blade

The content blade looks for matches to the Prince Edward Island driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as PE or Prince Edward Island in a close proximity.

License pattern rules: 5 - 6 digits

Driver's license pattern:

- *DDDD*
- *DDDDDD*

Protected Health Information Terms Content Blade

The content blade looks for words and phrases related to personal health records and health insurance claims.

The content blade will match with a combination of the following pieces of information, either:

1 More than one match to the Protected Health Information dictionary

2 A single match to the Protected Health Information dictionary plus two of either a name, U.S. Address or U.S. Date

3 A single match to the Protected Health Information dictionary with a patient or doctor identification word or phrase (e.g. patient ID, physician name)

Quebec Drivers Licence Content Blade

The content blade looks for matches to the Quebec driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as QC or Quebec in a close proximity.

License pattern rules: 1 letter followed by 12 digits

Driver's license pattern: LDDDDDDDDDDDD

Rhode Island License Number Content Blade

The content blade looks for matches to the Rhode Island driver's license pattern and words and phrases such as driver's license and license number and terms such as RI or Rhode Island.

Driver's license pattern: 7 Numeric

Saskatchewan Drivers Licence Content Blade

The content blade looks for matches to the Saskatchewan driver's license pattern and words and phrases such as driver's licence and permis de conduire plus terms such as SK or Saskatchewan in a close proximity.

License pattern rules: 8 digits

License pattern: *DDDDDDDD*

SIN Formatted Content Blade

The content blade looks for formatted patterns of the Canadian Social Insurance number (SIN).

The content blade will match with a combination of the following pieces of information in medium proximity, either:

1 More than one match to a formatted SIN

2 A single match to a formatted SIN plus a driver's license or date of birth word or phrase

3 A single match to a formatted SIIN with word or p

SIN Unformatted Content Blade

The content blade looks for unformatted patterns of the Canadian Social Insurance (SIN). The content blade will match if an unformatted SIN is found within close proximity of a word or phrase for a Social Insurance number (e.g. Social Insurance, SIN) or driver's license or date of birth.

SSN Formatted Content Blade

SSN Formatted Content Blade

The content blade will match with a combination of the following pieces of information in medium proximity, either:

- More than one match to a formatted SSN
- A single match to a formatted SSN plus two of either a name, U.S. Address or U.S. Date
- A single match to a formatted SSN with word or phrase for a Social Security number (e.g. Social Security, SSN)

SSN Unformatted Content Blade

The content blade looks for unformatted patterns of the U.S. Social Security number (SSN). The content blade will match if an unformatted SSN is found within close proximity of a word or phrase for a Social Security number (e.g. Social Security, SSN).

South Carolina License Number Content Blade

The content blade looks for matches to the South Carolina driver’s license pattern and words and phrases such as driver’s license and license number and terms such as SC or South Carolina.

Driver's license pattern: 9 Numeric

South Dakota License Number Content Blade

The content blade looks for matches to the South Dakota driver’s license pattern and words and phrases such as driver’s license and license number and terms such as SD or South Dakota.

Driver's license pattern: 8 Numeric; or Social Security Number

Spain National Identification Number Content Blade

The content blade looks for matches to the Spain National Identification Number entity and words and phrases such as Documento Nacional de Identidad and Número de Identificación de Extranjeros. It also uses regular expressions to differentiate between telephone numbers and to prevent double counting of DNIs and NIEs without check letters.

Spain Passport Number Content Blade

The content blade looks for matches to the Spain Passport Number and words and phrases such as pasaporte or passport.

Passport Rule: 8 alphanumeric characters -- 2 letters followed by 6 digits.

Pattern:

LLDDDDDD

LL-DDDDDD

LL DDDDDD

Spain Social Security Number Content Blade

The content blade requires the following to match for a Spain Social Security number in a close proximity.

1 Spain Social Security number

2 Words or phrases for a social security number (e.g. número de la seguridad social, social security number)

Sweden IBAN Number Content Blade

The content blade requires the following to match for a Sweden IBAN number in a close proximity.

1 IBAN words and phrases (e.g. International Bank Account Number, IBAN

2 Sweden IBAN number pattern

IBAN Rule: SE country code followed by 22 digits.

Pattern: SE DDDDDDDDDDDDDDDDDDDDDD

Sweden Passport Number Content Blade

The content blade looks for matches to the Sweden Passport Number regular expression with the following possible combinations of supporting evidence.

1 Words and phrases for passport such as Passnummer

2 Words and phrases for the country Sweden, nationality and expiry dates

Passport Rule: 8 digits

Pattern:

DDDDDDDD

DD-DDDDDD

LL-DDDDDD

Tennessee License Number Content Blade

The content blade looks for matches to the Texas driver's license pattern and words and phrases such as driver's license and license number and terms such as TX or Texas.

Driver's license pattern: 8 Numeric

UK BIC Number Content Blade

The content blade scans for UK BIC numbers by requiring matches for both rules.

1 European BIC number format

2 UK format of the BIC number

BIC rule: 8 or 11 alphanumeric characters. Letters 5th and 6th will always have "GB" as the ISO 3166-1 alpha-2 country code.

Pattern:

LLLLLLAAA

LLLLLLAAAAA

LLLLLLAA-AAA

LLLLLLAA AAA

LLLLLL AA AAA

LLLL LL AA AAA

LLLL LL AA-AAA

UK Driving License Number Content Blade

The content blade requires the following to match for a UK driving license in a close proximity.

1 UK driving license pattern

2 Either words or phrases for a driving license (e.g. driving license) or personal identification (e.g. date of birth, address, telephone)

Driving license rule: 16 - 18 alphanumeric characters and begins with a letter.

Pattern:

LAAAADDDDDDLLDLLDD

Some digits are limited in the values accepted.

UK IBAN Number Content Blade

The content blade requires the following to match for a UK IBAN number in a close proximity.

1 European IBAN number format

2 UK IBAN number pattern

IBAN Rule: "GB" country code followed by 20 characters.

GB, ISO country code

2 Digits (numeric characters 0 to 9 only) , Check Digits (IBAN)

4 Upper case letters (A-Z only), Bank Identifier Digits

6 Digits (numeric characters 0 to 9 only), Bank branch code

8 Digits (numeric characters 0 to 9 only), Account number

Pattern:

GBDDLLLLDDDDDDDDDDDDD

GB DD LLLL DDDD DDDD DDDD DD

GB DD LLLL DDDDDD DDDDDDDD

UK National Health Service Number Content Blade

The content blade requires the following to match for a UK National Health Service number in a close proximity.

1 UK National Health Service number format

2 Words and phrases relating to the National Health Service or patient identification or date of birth

UK NINO Formal Content Blade

The content blade looks for the formal pattern of the UK National Insurance number (NINO).

The content blade will match with a combination of the following pieces of information in high proximity, either:

1 More than one match to a NINO formal pattern

2 A single match to a NINO formal with word or phrase for a National Insurance number (e.g. NINO, taxpayer number)

UK Passport Number Content Blade

The content blade looks for matches to one of the U.K. passport number entities with the following supporting evidence.

1 Words and phrases for passport such as passport or a national passport code preceding a passport number

2 Words and phrases for the country, U.K, or the date of issue (optional match)

Utah License Number Content Blade

The content blade looks for matches to the Utah driver's license pattern and words and phrases such as driver's license and license number and terms such as UT or Utah.

Driver's license pattern: 6 - 10 Numeric

Virginia License Number Content Blade

The content blade looks for matches to the Virginia driver's license pattern and words and phrases such as driver's license and license number and terms such as VA or Virginia.

Driver's license pattern: 1 Alphabetic, 8 Numeric

Visa Card Number Content Blade

The content blade looks for a combination of the following pieces of information, either:

1 More than one JCB credit card number

2 A single credit card number plus words and phrases such as ccn, credit card, expiration date

3 A single credit card number plus an expiration date

Washington License Number Content Blade

The content blade looks for matches to the Washington driver's license pattern and words and phrases such as driver's license and license number and terms such as WA or Washington.

Driver's license pattern: 5 Alphabetic (last name), 1 Alphabetic (first name), 1 Alphabetic (middle name), 3 Numeric, 2 Alphanumeric. If last or middle name field falls short, fill with *s.

Wisconsin License Number Content Blade

The content blade looks for matches to the Wisconsin driver's license pattern and words and phrases such as driver's license and license number and terms such as WI or Wisconsin.

Driver's license pattern: 1 Alphabetic, 13 Numeric

Wyoming License Number Content Blade

The content blade looks for matches to the Wyoming driver's license pattern and words and phrases such as driver's license and license number and terms such as WY or Wyoming.

Driver's license pattern: 9 - 10 Numeric

Supported File Formats

vShield Data Security can detect the following file formats.

Table 15-2. Archive Formats

Application Format	Extensions
7-Zip 4.57	7Z
BinHex	HQX
BZIP2	BZ2
Expert Witness (EnCase)Compression Format	E0, E101 etc
GZIP 2	GZ
ISO-9660 CD Disc Image Format	ISO
Java Archive	JAR
Legato EMailXtender Archive	EMX
MacBinary	BIN
Mac Disk copy Disk Image	DMG
Microsoft Backup File	BKF
Microsoft Cabinet Format 1.3	CAB
Microsoft Compressed Folder	LZH LHA
Microsoft Entourage	
Microsoft Outlook Express	DBX
Microsoft Outlook Offline Store 2007	OST
Microsoft Outlook Personal Store 2007	PST
OASIS Open Document Forma	ODC SXC STC ODT SXW STW
Open eBook Publication Structure	EPUB
PKZIP	ZIP
RAR archive	RAR
Self-extracting Archives	SEA
Shell Scrap Object File	SHS
Tape Archive	TAR
UNIX Compress	Z

Table 15-2. Archive Formats (Continued)

Application Format	Extensions
UUEncoding	UUE
WinZip	ZIP

Table 15-3. Computer-Aided Design Formats

Application Format	Extensions
CATIA formats 5	CAT
Microsoft Visio 5, 2000, 2002, 2003, 2007	VSD
MicroStation 7, 8	DGN
Omni Graffle	GRAFFLE

Table 15-4. Database Formats

Application Format	Extensions
Microsoft Access 95, 97, 2000, 2002, 2003, 2007	MDB

Table 15-5. Display Formats

Application Format	Extensions
Adobe PDF 1.1 to 1.7	PDF

Table 15-6. Mail Formats

Application Format	Extensions
Domino XML Language	DXL
Legato Extender	ONM
Lotus Notes database 4, 5, 6.0, 6.5, 7.0, and 8.0	NSF
Mailbox Thunderbird 1.0 and Eudora 6.2	MBX
Microsoft Outlook 97, 2000, 2002, 2003, and 2007	MSG
Microsoft Outlook Express Windows 6 and MacIntosh 5	EML
Microsoft Outlook Personal Folder 97, 2000, 2002, and 2003	PST
Text Mail (MIME)	Various

Table 15-7. Multimedia Formats

Application Format	Extensions
Advanced Streaming Format 1.2	DXL

Table 15-8. Presentation Formats

Application Format	Extensions
Apple iWork Keynote 2, 3, ‘08, and ‘09	GZ
Applix Presents 4.0, 4.2, 4.3, 4.4	AG
Corel Presentations 6, 7, 8, 9, 10, 11, 12, and X3	SHW

Table 15-8. Presentation Formats (Continued)

Application Format	Extensions
Lotus Freelance Graphics 2	PRE
Lotus Freelance Graphics 96, 97, 98, R9, and 9.8	PRZ
Macromedia Flash through 8.0	SWF
Microsoft PowerPoint PC 4	PPT
Microsoft PowerPoint Windows 95, 97, 2000, 2002, and 2003	PPT, PPS, POT
Microsoft PowerPoint Windows XML 2007	PPTX, PPTM, POTX, POTM, PPSX, and PPSM
Microsoft PowerPoint Macintosh 98, 2001, v.X, and 2004	PPT
OpenOffice Impress 1 and 1.1	SXP
StarOffice Impress 6 and 7	SXP

Table 15-9. Spreadsheet Formats

Application Format	Extensions
Apple iWork Numbers '08 and 2009	GZ
Applix Spreadsheets 4.2, 4.3, and 4.4	AS
Comma Separated Values	CSV
Corel Quattro Pro 5, 6, 7, 8, X4	WB2. WB3, QPW
Data Interchange Format	DIF
Lotus 1-2-3 96, 97, R9, 9.8, 2, 3, 4, 5	123, WK4
Lotus 1-2-3 Charts 2, 3, 4, 5	123
Microsoft Excel Windows 2.2 through 2003	XLS, XLW, XLT, XLA
Microsoft Excel Windows XML 2007	XLSX, XLTX, XLSM, XLTM, XLAM
Microsoft Excel Charts 2, 3, 4, 5, 6, 7	XLS
Microsoft Excel Macintosh 98, 2001, v.X, 2004	XLS
Microsoft Office Excel Binary Format 2007	XLSB
Microsoft Works Spreadsheet 2, 3, 4	S30 S40
Oasis Open Document Format 1, 2	ODS, SXC, STC
OpenOffice Calc 1, 1.1	SXC, ODS, OTS
StarOffice Calc 6, 7	

Table 15-10. Text and Markup Formats

Application Format	Extensions
ANSI	TXT
ASCII	TXT
Extensible Forms Description Language	XFDL, XFD
HTML 3, 4	HTM, HTML
Microsoft Excel Windows XML 2003	XML
Microsoft Word Windows XML 2003	XML
Microsoft Visio XML 2003	vdx

Table 15-10. Text and Markup Formats (Continued)

Application Format	Extensions
MIME HTML	MHT
Rich Text Format 1 through 1.7	RTF
Unicode Text 3, 4	TXT
XHTML 1.0	HTM, HTML
XML (generic)	XML

Table 15-11. Word Processing Formats

Application Format	Extensions
Adobe FrameMaker InterchangeFormat 5, 5.5, 6, 7	MIF
Apple iChat Log AV, AV 2, AV 2.1,AV 3	LOG
Apple iWork Pages '08, 2009	GZ
Applix Words 3.11, 4, 4.1, 4.2, 4.3,4.4	AW
Corel WordPerfect Linux 6.0, 8.1	WPS
Corel WordPerfect Macintosh 1.02, 2, 2.1, 2.2, 3, 3.1	WPS
Corel WordPerfect Windows 5, 5.1, 6, 7, 8, 9, 10, 11, 12, X3	WO, WPD
DisplayWrite 4	IP
Folio Flat File 3.1	FFF
Founder Chinese E-paper Basic 3.2.1	CEB
Fujitsu Oasys 7	OA2
Haansoft Hangul 97, 2002, 2005, 2007	HWP
IBM DCA/RFT (Revisable Form Text) SC23-0758 -1	DC
JustSystems Ichitaro 8 through 2009	JTD
Lotus AMI Pro 2, 3	SAM
Lotus AMI Professional Write Plus 2.1	AMI
Lotus Word Pro	96, 97, R9
Lotus SmartMaster 96, 97	MWP
Microsoft Word PC 4, 5, 5.5, 6	DOC
Microsoft Word Windows 1.0 and 2.0, 6, 7, 8, 95, 97, 2000, 2002, 2003	DOC
Microsoft Word Windows XML 2007	DOCX, DOTX, DOTM
Microsoft Word Macintosh 4, 5, 6, 98, 2001, v.X, 2004	DOC
Microsoft Works 2, 3, 4, 6, 2000	WPS
Microsoft Windows Write 1, 2, 3	WRI
Oasis Open Document Format 1, 2	ODT, SXW, STW
OpenOffice Writer 1, 1.1	SXW, ODT
Omni Outliner 3	OPML, OO3, OPML, OOUTLINE
Skype Log File	DBB
StarOffice Writer 6, 7	SXW, ODT
WordPad through 2003	RTF

Table 15-11. Word Processing Formats (Continued)

Application Format	Extensions
XML Paper Specification	XPS
XyWrite 4.12	XY4

Troubleshooting 16

This section guides you through troubleshooting common vShield issues.

This chapter includes the following topics:

- "Troubleshoot vShield Manager Installation," on page 229
- "Troubleshooting Operational Issues," on page 230
- "Troubleshooting vShield Edge Issues," on page 231
- "Troubleshoot vShield Endpoint Issues," on page 233
- "Troubleshooting vShield Data Security Issues," on page 234

Troubleshoot vShield Manager Installation

This section provides details on how to troubleshoot vShield Manager installation.

vShield OVA File Cannot Be Installed in vSphere Client

You cannot install the vShield OVA file.

Problem

When I try to install the vShield OVA file, the install fails.

Solution

If a vShield OVA file cannot be installed, an error window in the vSphere Client notes the line where the failure occurred. Send this error information with the vSphere Client build information to VMware technical support.

Cannot Log In to CLI After the vShield Manager Virtual Machine Starts

Problem

I cannot log in to the vShield Manager CLI after I installed the OVF.

Solution

Wait a few minutes after completing the vShield Manager installation to log in to the vShield Manager CLI. In the Console tab view, press Enter to check for a command prompt if the screen is blank.

Cannot Log In to the vShield Manager User Interface

Problem

When I try to log in to the vShield Manager user interface from my Web browser, I get a Page Not Found exception.

Solution

The vShield Manager IP address is in a subnet that is not reachable by the Web browser. The IP address of the vShield Manager management interface must be reachable by the Web browser to use vShield.

Troubleshooting Operational Issues

Operational issues are problems that might arise after installation.

vShield Manager Cannot Communicate with a vShield App

Problem

I cannot configure a vShield App from the vShield Manager.

Solution

If you cannot configure the vShield App from the vShield Manager, there is a break in connectivity between the two virtual machines. The vShield management interface cannot talk to the vShield Manager management interface. Make sure that the management interfaces are in the same subnet. If VLANs are used, make sure that the management interfaces are in the same VLAN.

Another reason could be that the vShield App or vShield Manager virtual machine is powered off.

Cannot Configure a vShield App

Problem

I cannot configure a vShield App.

Solution

This might be the result of one of the following conditions.

- The vShield App virtual machine is corrupt. Uninstall the offending vShield App from the vShield Manager user interface. Install a new vShield App to protect the ESX host.
- The vShield Manager cannot communicate with the vShield App.
- The storage/LUN hosting the vShield configuration file has failed. When this happens, you cannot make any configuration changes. However, the firewall continues to run. You can store vShield virtual machines to local storage if remote storage is not reliable.

Take a snapshot or create a TAR of the affected vShield App by using the vSphere Client. Send this information to VMware technical support.

Firewall Block Rule Not Blocking Matching Traffic

Problem

I configured an App Firewall rule to block specific traffic. I used Flow Monitoring to view traffic, and the traffic I wanted to block is being allowed.

Solution

Check the ordering and scope of the rule. This includes the container level at which the rule is being enforced. Issues might occur when an IP address-based rule is configured under the wrong container.

Check where the affected virtual machine resides. Is the virtual machine behind a vShield App? If not, then there is no agent to enforce the rule. Select the virtual machine in the resource tree. The App Firewall tab for this virtual machine displays all of the rules that affect this virtual machine.

Place any unprotected virtual machines onto a vShield-protected switch or protect the vSwitch that the virtual machine is on by installing a vShield.

Enable logging for the App Firewall rule in question. This might slow network traffic through the vShield App.

Verify vShield App connectivity. Check for the vShield App being out of sync on the System Status page. If out of sync, click **Force Sync**. If it is still not in sync, go to the System Event log to determine the cause.

No Flow Data Displaying in Flow Monitoring

Problem

I have installed the vShield Manager and a vShield App. When I opened the Flow Monitoring tab, I did not see any data.

Solution

This might be the result of one or more of the following conditions.

- You did not allow enough time for the vShield App to monitor traffic sessions. Allow a few minutes after vShield App installation to collect traffic data. You can request data collection by clicking **Get Latest** on the Flow Monitoring tab.
- Traffic is destined to virtual machines that are not protected by a vShield App. Make sure your virtual machines are protected by a vShield App. Virtual machines must be in the same port group as the vShield App protected (p0) port.
- There is no traffic to the virtual machines protected by a vShield App.
- Check the system status of each vShield App for out-of-sync issues.

Troubleshooting vShield Edge Issues

This section provides details on how to troubleshoot vShield Edge operational issues.

Virtual Machines Are Not Getting IP Addresses from the DHCP Server

Procedure

1 Verify DHCP configuration was successful on the vShield Edge by running the CLI command: `show configuration dhcp`.

2 Check whether DHCP service is running on the vShield Edge by running CLI command: `show service dhcp`

3 Ensure that vmnic on virtual machine and vShield Edge is connected (**vCenter > Virtual Machine > Edit Settings > Network Adapter > Connected/Connect at Power On** check boxes).

When both a vShield App and vShield Edge are installed on the same ESX host, disconnection of NICs can occur if a vShield App is installed after a vShield Edge.

Load-Balancer Does Not Work

Procedure

1 Verify that the Load balancer is running by running the CLI command: `show service lb`.

Load balancer can be started by issuing the `start` command.

2 Verify the load-balancer configuration by running command: `show configuration lb`.

This command also shows on which external interfaces the listeners are running.

Load-Balancer Throws Error 502 Bad Gateway for HTTP Requests

This error occurs when the backend or Internal servers are not responding to requests.

Procedure

1 Verify that internal server IP addresses are correct.

The current configuration can be seen through the vShield Manager or through the CLI command `show configuration lb`.

2 Verify that internal server IP addresses are reachable from the vShield Edge internal interface.

3 Verify that internal servers are listening on the IP:Port combination specified at the time of load balancer configuration.

If no port is specified, then IP:80 must be checked. The internal server must not listen on only 127.0.0.1:80; either 0.0.0.0:80 or <internal-ip>:80 must be open.

VPN Does Not Work

Procedure

1 Verify that the other endpoint of the tunnel is configured correctly.

Use the CLI command: `show configuration ipsec`

2 Verify that IPSec service is running on the vShield Edge.

To verify using the CLI command: `show service ipsec`. IPSec service has to be started by issuing the `start` command.

If ipsec is running and any errors have occurred at the time of tunnel establishment, the output of `show service ipsec` displays relevant information.

3 Verify the configuration at both ends (vShield Edge and remoteEnd), notably the shared keys.

4 Debug MTU or fragmentation related issues by using ping with small and big packet sizes.

- `ping –s 500 ip–at–end–of–the–tunnel`
- `ping –s 2000 ip–at–end–of–the–tunnel`

SSL VPN does Not Work

Procedure

1 Ensure that SSL VPN and Load Balancer are not configured on the same host.

2 Verify that the SSL VPN service is enabled.

3 Verify that the server settings have been specified to enable SSL on a vShield Edge interface.

4 Ensure that the external authentication server is reachable.

Troubleshoot vShield Endpoint Issues

This section provides details on how to troubleshoot vShield Endpoint operational issues.

Thin Agent Logging

vShield Endpoint thin agent logging is done inside the protected virtual machines. Two registry values are read at boot time from the windows registry. They are polled again periodically.

The two registry values, `log_dest` and `log_level` are located in the following registry locations:

- `HKLM\System\CurrentControlSet\Services\vsepflt\Parameters\log_dest`
- `HKLM\System\CurrentControlSet\Services\vsepflt\Parameters\log_level`

Both are `DWORD` bit masks that can be any combination of the following values:

Table 16-1. Thin Agent Logging

DWORD	Value	Description
`log_dest`	`0x1`	`WINDBLOG`
	`0x2`	Requires debug mode `VMWARE_LOG` Log file is stored in the root directory of the virtual machine
`log_level`	`0x1`	`AUDIT`
	`0x2`	`ERROR`
	`0x4`	`WARN`
	`0x8`	`INFO`
	`0x10`	`DEBUG`

By default, the values in release builds are set to VMWARE_LOG and AUDIT. You can Or the values together.

For more on monitoring vShield Endpoint health, see Chapter 14, “vShield Endpoint Events and Alarms,” on page 179.

Component Version Compatibility

The SVM version and the thin agent version must be compatible.

To retrieve version numbers for the various components, do the following:

- SVM: For partner SVMs, refer to the instructions from the from the anti-virus solution provider. For the vShield Data Security virtual machine, log in to the vShield Manager and select the virtual machine from the inventory. The Summary tab displays the build number.

- GVM: Right-click on the properties of the driver files to get the build number. The path to the driver is `C:\WINDOWS\system32\drivers\vsepflt.sys`.
- vShield Endpoint Module: Log in to the vShield Manager and select a host from the inventory. The Summary tab displays the vShield Endpoint build number.

Check vShield Endpoint Health and Alarms

The vShield Endpoint components should be able to communicate with the vShield Manager.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a datacenter, cluster, or ESX host from the resource tree.

3 Click the **vShield App** tab.

4 Click **Endpoint.**

5 Confirm that the security virtual machine (SVM), the ESX host-resident vShield Endpoint module, and the protected virtual machine-resident thin agent are normal.

6 If the virtual machine-resident thin agent is not normal, check that the version of VMware Tools is 8.6.0 (released with ESXi 5.0 Patch 1).

7 If an alarm is displayed, take appropriate action. For more information, see "vShield Endpoint Alarms," on page 180.

Troubleshooting vShield Data Security Issues

Since vShield Data Security uses the vShield Endpoint technology, troubleshooting is very similar for both components.

When you come across any vShield Data Security issue, first ensure that the Data Security appliance is reported as enabled. Then verify that a data security scan was started.

Review Scan Start and Stop Timestamp

vShield Data Security only scans those virtual machines that are powered on. The first step in troubleshooting vShield Data Security issues is to confirm that the virtual machine was scanned.

Procedure

1 In the vSphere Client, go to **Inventory > Hosts and Clusters**.

2 Select a datacenter, ESX host, or virtual machine from the resource tree.

3 Select the **Tasks and Events** tab.

4 Look for Scan in the Name column and confirm that it completed successfully.

About Accuracy in Detecting Violations

Accuracy is measured by two factors: recall and precision. Taken together, the ideal mix of recall and precision will ensure that you get the content that you need to secure and nothing else. Any content detection is evaluated in two ways: positive or negative, and true or false (e.g., did I identify what I was looking for, and was my identification correct?).

There are four possible outcomes that have the following meanings.

Table 16-2. Outcomes of Content Detection

	Positive	Negative
True	Sensitive content correctly identified as sensitive.	Non-sensitive content correctly identified as non-sensitive.
False	Non-sensitive content mistakenly identified as sensitive.	Sensitive content mistakenly identified as non-sensitive.

Recall gathers the fraction of the documents that are relevant to the content blade.

- High recall casts a wide net, and gathers all potentially sensitive documents. Too high a recall can result in more false positives. [False positive = a document judged sensitive by the content blade, which is not, in fact, sensitive.]
- Low recall is more selective in the documents returned as sensitive. Too low a recall can result in more false negatives. [False negative = a document judged not to be sensitive by the content blade, but which IS, in fact, sensitive.]

Precision is the percent of retrieved documents that are relevant to the search.

- High precision can reduce the number of false positives returned.
- Low precision can increase the number of false positives returned.

Precision refers to the relevancy of the results returned. For example, did all of the documents that triggered the Payment Card Industry Data Security Standard (PCI DSS) policy contain actual credit card numbers, or did some contain UPC or EAN numbers which were incorrectly identified as sensitive PCI data? High precision can be achieved with a narrow, focused search to make sure that every piece of content that is caught is truly sensitive.

Table 16-3. Precision and Recall

Accuracy Factor	Measurement	Problem if Value is Low
Precision	The percentage of retrieved documents that are actually relevant.	Increased false
Recall	The percentage of all of the sensitive documents that are actually retrieved.	Increased false negatives

Index

A

add, service **27**
admin user account **39**
alarms for vShield Endpoint **180**
App Firewall
  about L4 and L2/L3 rules **168**
  adding L4 rules **169**
  adding rules from Flow Monitoring **164**
  change order of rule **173**
  Default Rules **168**
  deleting rules **172**
  hierarchy of rules **168**
  planning rule enforcement **169**
  revert to previous rule **173**
appliance
  add **68**
  delete **69**
  edit **69**
Audit Logs **34, 51**
audit messages for vShield Endpoint **181**

B

Backups
  on-demand **45**
  restoring **46**
  scheduling **46**

C

Cluster Level Rules **168**
content blades
  ABA Routing Number **204**
  Admittance and Discharge Dates Content Blade **204**
  Alabama Drivers License Content Blade **204**
  Alaska Drivers License Content Blade **204, 205**
  Alberta Drivers Licence Content Blade **204, 205**
  American Express Content Blade **205**
  Arizona Drivers License Content Blade **205**
  Arkansas Drivers License Content Blade **204, 205**
  Australia Bank Account Number Content Blade **205**
  Australia Business Number Content Blade **206**
  Australia Company Number Content Blade **206**
  Australia Medicare Card Number Content Blade **206**
  Australia Tax File Number Content Blade **206**
  California Drivers License Number Content Blade **206**
  Canada Drivers License Number Content Blade **206**
  Canada Social Insurance Number Content Blade **206**
  Colorado Drivers License Number Content Blade **206**
  Connecticut Drivers License Number Content Blade **207**
  Credit Card Track Data Content Blade **207**
  Custom Account Number Content Blade **207**
  Delaware Drivers License Number Content Blade **207**
  EU Debit Card Number Content Blade **207**
  Florida Drivers License Number Content Blade **208**
  France BIC Number Content Blade **208**
  France Driving License Number Content Blade **208**
  France National Identification Number Content Blade **208**
  France VAT Number Content Blade **208**
  Georgia Drivers License Number Content Blade **208**
  Germany BIC Number Content Blade **208**
  Germany Driving License Number Content Blade **209**
  Germany National Identification Numbers Content Blade **209**
  Germany Passport Number Content Blade **209**
  Germany VAT Number Content Blade **209**
  Group Insurance Numbers Content Blade **209**
  Hawaii Drivers License Number Content Blade **209**
  Idaho Drivers License Number Content Blade **210**
  Illinois Drivers License Number Content Blade **210**
  Index of Procedures Content Blade **211**

Indiana Drivers License Number Content Blade **210**
Iowa Drivers License Number Content Blade **211**
Italy Driving License Number Content Blade **211**
Italy IBAN Number Content Blade **211**
Italy National Identification Numbers Content Blade **209**
ITIN Unformatted Content Blade **212**
Kansas Drivers License Number Content Blade **212**
Kentucky Drivers License Number Content Blade **212**
Louisiana Drivers License Number Content Blade **212**
Maine Drivers License Number Content Blade **212**
Manitoba Drivers Licence Content Blade **212**
Maryland Drivers License Number Content Blade **213**
Michigan Drivers License Number Content Blade **213**
Minnesota Drivers License Number Content Blade **213**
Mississippi Drivers License Number Content Blade **213**
Missouri Drivers License Number Content Blade **213**
Montana Drivers License Number Content Blade **214**
NDC Formulas Dictionary Content Blade **214**
Nebraska Drivers License Number Content Blade **214**
Netherlands Driving Licence Number Content Blade **214**
Netherlands IBAN Number Content Blade **214**
Netherlands National Identification Numbers Content Blade **215**
Netherlands Passport Number Content Blade **215**
New Brunswick Drivers Licence Content Blade **215**
New Hampshire Drivers License Number Content Blade **215**
New Jersey Drivers License Number Content Blade **215**
New Mexico Drivers License Number Content Blade **216**
New York Drivers License Number Content Blade **216**
New Zealand Health Practitioner Index Number Content Blade **216**
New Zealand Inland Revenue Department Number **216**
New Zealand National Health Index Number Content Blade **216**
Newfoundland and Labrador Drivers Licence Content Blade **216**
North Carolina Drivers License Number Content Blade **216**
North Dakota Drivers License Number Content Blade **216**
Nova Scotia Drivers Licence Content Blade **217**
Ohio Drivers License Number Content Blade **217**
Oklahoma License Number Content Blade **217**
Ontario Drivers Licence Content Blade **217**
Oregon License Number Content Blade **217**
Patient Identification Numbers Content Blade **217**
Pennsylvania License Number Content Blade **217**
Prince Edward Island Drivers Licence Content Blade **217**
Protected Health Information Terms Content Blade **218**
Quebec Drivers Licence Content Blade **218**
Rhode Island License Number Content Blade **218**
Saskatchewan Drivers Licence Content Blade **218**
SIN Formatted Content Blade **218**
SIN Unformatted Content Blade **219**
South Carolina License Number Content Blade **219**
South Dakota License Number Content Blade **219**
Spain National Identification Number Content Blade **219**
Spain Passport Number Content Blade **219**
Spain Social Security Number Content Blade **220**
SSN Formatted Content Blade **219**
SSN Unformatted Content Blade **219**
Sweden IBAN Number Content Blade **220**
Sweden Passport Number Content Blade **220**
Tennessee License Number Content Blade **220**
UK Driving License Number Content Blade **221**
UK IBAN Number Content Blade **221**
UK NINO Formal Content Blade **222**
UK Passport Number Content Blade **222**
Utah License Number Content Blade **222**
Virginia License Number Content Blade **222**
Visa Card Number Content Blade **222**

Washington License Number Content Blade **222**
Wisconsin License Number Content Blade **222**
Wyoming License Number Content Blade **223**

D

data
on-demand backups **45**
restoring a backup **46**
scheduling backups **46**
Data Center High Precedence Rules **168**
Data Center Low Precedence Rules **168**
Data Security,policy,regulations **184**
Data Security,user roles **183**
date **24**
date range for Flow Monitoring **165**
Default Rules **168**
delete
service manager **155**
service profile **156**
delete service **155**
deleting a user **42**
DNS **23**

E

editing a user account **41**
events
sending to syslog **157**
syslog format **51**
vShield App **50**
vShield Manager **49**
events for vShield Endpoint **180**

F

firewall
adding L4 rules **169**
adding rules from Flow Monitoring **164**
App Firewall, about **167**
deleting rules **172**
planning rule enforcement **169**
flow analysis date range **165**
Flow Monitoring
adding an App Firewall rule **164**
date range **165**
Force Sync **158**

G

GUI, logging in **19**

H

hierarchy of App Firewall rules **168**
high availability **145**
host alarms for vShield Endpoint **180**
Hosts & Clusters view **20**

I

installing, updates **43**
inventory panel **20**
IPSec service
delete **89**
disable **90**
enable **89**
IPSec VPN
add **87**
configuration examples **90**
edit **88**
enable **88**
overview **86**

L

L2/L3 rules, about **168**
L4 rules
about **168**
adding **169**
load balancer, add pool **140**
Load Balancer **140**
login, vShield Manager **19**
logs
audit **34, 51**
technical support **25**

M

Massachusetts Drivers License Number Content Blade **213**

N

namespace **167**
NAT **81**
network scope, view and edit **60**
Networks view **20**
NSX Edge, SSL VPN overview **109**
NTP **24**

P

password **41**
plug-in **24**

R

redeploy vShield Edge **149**
regulations
ABA Routing Numbers **189**
Arizona SB-1338 **188**
Australia Bank Account Numbers **189**
Australia Medicare Card Numbers **190**
Australia Tax File Numbers **190**
California AB-1298 **190**

California SB-1386 **191**
Canada Drivers License Numbers **191**
Canada Social Insurance Numbers **191**
Colorado HB-1119 **192**
Connecticut SB-650 **192**
Credit Card Numbers **192**
Custom Account Numbers **192**
EU Debit Card Numbers **193**
FERPA (Family Educational Rights and Privacy Act) **193**
Florida HB-481 **193**
France IBAN Numbers Policy **193**
France National Identification Numbers Policy **193**
Georgia SB-230 Policy **194**
Germany BIC Numbers Policy **194**
Germany Driving License Numbers Policy **194**
Germany IBAN Numbers Policy **194**
Germany National Identification Numbers Policy **194**
Germany VAT Numbers Policy **194**
Hawaii SB-2290 Policy **195**
HIPPA (Healthcare Insurance Portability and Accountability Act) Policy **195**
Idaho SB-1374 Policy **195**
Illinois SB-1633 **196**
Indiana HB-1101 Policy **196**
Italy Driving License Numbers Policy **196**
Italy IBAN Numbers Policy **196**
Italy National Identification Numbers Policy **196**
Kansas SB-196 Policy **197**
Louisiana SB-205 Policy **197**
Maine LD-1671 Policy **197**
Massachusetts CMR-201 **198**
Minnesota HF-2121 **198**
Montana HB-732 Policy **198**
Netherlands Driving Licence Numbers **198**
Nevada SB-347 **199**
New Hampshire HB-1660 **199**
New Jersey A-4001 **199**
New York AB-4254 **200**
New Zealand Inland Revenue Department Numbers **200**
New Zealand Ministry of Health Numbers **200**
Ohio HB-104 **200**
Oklahoma HB-2357 **201**
Patient Identification Numbers **201**
Payment Card Industry Data Security Standard (PCI-DSS) **201**
Texas SB-122 **201**
UK BIC Numbers **202**
UK Driving Licence Numbers **202**
UK IBAN Numbers **202**
UK National Health Service Numbers **202**
UK National Insurance Numbers (NINO) **202**
UK Passport Numbers **202**
US Drivers License Numbers Policy **203**
US Social Security Numbers **203**
Utah SB-69 **203**
Vermont SB-284 **203**
Washington SB-6043 **203**
reports
  audit log **34, 51**
  system events **49**
restarting a vShield App **158**
restoring backups **46**
roles and rights, about **38**
rules
  adding L4 rules to App Firewall **169**
  deleting App Firewall rules **172**

S

scheduling backups **46**
Secure Port Group Rules **168**
Secured Port Groups view **20**
security groups
  about **168**
  add **34**
server pool
  delete **144**
  edit **143**
service
  add **27**
  delete **155**
service manager, delete **155**
service profile, delete **156**
services
  DNS **23**
  NTP **24**
single sign on **37**
SpoofGuard **174**
SSL VPN-plus, authentication, add **112, 119**
SSL certificate **26**
SSL VPN
  client configuration **134**
  edit general settings **138**
  edit portal design **139**
    login/logoff script
      add **135**
      delete **136**
      disable **137**
      edit **135**
      enable **136**

login/logoff scripts
change the order of **138**
refresh **137**
logs **138**
web resource **118**
SSL VPN-Plu, IP pool, change order of **128**
SSL VPN-Plus
add installation package **115, 131**
add IP pool **111, 126**
add private network **111, 128**
add user **116, 118, 132**
enable **116, 125**
installation package
add **115, 131**
delete **132**
IP pool
add **111, 126**
delete **126**
disable **127**
edit **126, 127**
private network
change order of **130**
delete **129**
users
add **116, 118, 132**
change password **134**
delete **133**
edit **133**
SSL VPN,overview **109**
static route
add **83**
set default gateway **83**
status
of update **43**
vShield App **158**
vShield Edge **68**
vShield Endpoint **179**
supported file formats **223**
SVM alarms for vShield Endpoint **180**
syncing a vShield App **158**
syslog, vShield Edge **147**
syslog format **51**
Syslog Server **157**
System Events **49**
System Status
Force Sync **158**
Restart **158**
traffic stats **159**
system time **24**

T

tech support logs
vShield App **159**
vShield Edge **148**
technical support log **25**
test VXLAN virtual wire connectivity **58**
time **24**
traffic analysis date range **165**
traffic stats for a vShield App **159**
troubleshooting
operational issues **230**
vShield Edge issues **231**
vShield Endpoint issues **233**
vShield Manager installation **229**

U

Update Status **43**
Update User **41**
Updates
installing **43**
Update Status **43**
user interface, logging in **19**
Users
admin account **39**
changing a password **41**
deleting **42**
editing **41**
roles and rights **38**

V

views
Hosts & Clusters **20**
Networks **20**
Secured Port Groups **20**
virtual server
delete **144**
edit **144**
virtual wire
connect virtual machines to **57**
create **55**
test connectivity; **58**
VPN
configure service **87**
manage **86**
vShield
vShield App **15**
vShield Edge **15**
vShield Endpoint **15**
vShield Manager **15**
vShield App
about **15**
exclude virtual machines from protection **159**
fail safe mode **159**
forcing sync **158**
notification based on events **50**
restarting **158**
sending events to syslog server **157**

System Status **158**
traffic stats **159**
vShield Data Security
about **183**
policy **184**
scan **187**
supported file formats **223**
user roles **183**
vShield Edge
about **15**
add appliance **68**
add CA certificate **74**
add DHCP binding **85**
add DHCP IP pool **84**
add NAT rules **81**
certificate revocation list **75**
certificates **73**
client certificates **75**
configure CA signed certificate **73**
configure self signed certificate **74**
configure settings **68**
delete appliance **69**
DHCP **84**
DNS servers **146**
edit appliance **69**
firewall rules
add **76**
change priority **80**
delete **80**
edit **80**
manage **76**
force sync **148**
HA **146**
interface
delete **71**
disable **72**
edit **71**
Load Balancer **140**
static route; static route **83**
status **68**
syslog **147**
tech support logs **148**
VPN **86**
vShield Edge firewall rules, change default settings **79**
vShield Edgei, nterface, enable **72**
vShield Endpoint
about **15**
alarms **180**
audit messages **181**
events **180**
host alarms **180**
status **179**
SVM alarms **180**
vShield Manager
about **15**
date and time **24**
DNS **23**
inventory panel **20**
logging in **19**
notification based on events **49**
NTP **24**
on-demand backups **45**
restoring a backup **46**
scheduling a backup **46**
SSL Certificate **26**
Support **25**
system events **49**
user interface panels **20**
vSphere Plug-in **24**
vSphere Plug-in **24**
VXLAN virtual wire
add network scope **55**
assign segment ID pool & multicast address range **55**
associate clusters **54**
connect to vShield Edge **56**
deploy services **57**
edit **61**
network scope, contract **60, 61**
overview **53**
prepare for **54**
sample scenario **62**